Citizenship in the information society: protecting cyber-citizens from emerging problems through government regulation, ICT design and information ethics

Candice le Sueur

Candice le Sueur
African Centre of Excellence for Information Ethics
Department of Information Science, University of Pretoria
Candice.les@gmail.com

Abstract

Cyberspace is a space of enormous freedom which has been well used and badly abused. This paper considers options for dealing with current and emerging online problems by way of acknowledging the interconnectedness of the technical and social nature of cyberspace. Three main approaches are considered: regulation by governments or internet service providers; design approaches such as Anticipatory Technology Ethics, Value Sensitive Design and Artificial Moral Agents; and diffuse approaches of sensitisation by way of information ethics training. As a case in point, Pokemon Go will be referenced.

Keywords: Information ethics, government regulation, information and communication technologies, ethics in design, cyber-citizenship, Pokemon Go

Introduction

Both the nature of cyberspace and the way we, the community of cyber-citizens[1], have used and abused cyberspace, call for an intervention from information ethics. As cyber-citizens we have a dual-citizenship: we are citizens of our physical space (the Nation State for instance) and of cyberspace – a space that transcends physical environments[2]. Being citizens of cyberspace does allow us to transcend the oppressive or repressive parts of our physical environments to some degree (Schmidt and Cohen 2013), but that does not automatically mean that we may transcend the moral duties we have in life, whether in

physical space or cyberspace. Cyberspace is arguably the most ‘free space’ that humans collectively inhabit – albeit a virtual, man-made space. Eric Schmidt (Executive Chairman of Google) and Jared Cohen (Director of Google Ideas) have stated that the Internet is “the world’s largest ungoverned space” (2013: 3). There are less laws and regulations governing us here than anywhere else. Cyberspace has given humanity the greatest opportunity ever to have a clean slate to build a common (virtual) habitation where we can become more informed by both consuming and generating content (information).

Unfortunately, cyberspace also affords us the opportunities to both create new forms of social ills, and to recreate and entrench the social problems of the physical world. In the face of this great[3] freedom, we, the cyber-community, need to stand back and evaluate whether we have the courage and moral strength to enjoy this freedom responsibly. And although this freedom has created new ways for people to effectively mobilise themselves against what they see as repressive regimes[4], to become more informed on how to live healthy lifestyles, find support groups that transcend locality to address social and psychological problems, and to stay connected to friends and family in other parts of the world; we, the cyber-citizens, have also abused this freedom badly – as is seen in web pages that advocate the behaviours generally classified as psychiatric illness or disorders, the posting of perverse pornography (including the sexual abuse of children), platforms and forums for hate speech and incitement to violence, and the creation of new forms of threats to our privacy and security, as well as new methods of discrimination via online harassment.

The nature of cyberspace

Cyberspace has technical and social features that are inextricable from each other in its functioning, but possible to break down for the purpose of discussion.

The technical nature of cyberspace in very simple terms

While the term ‘cyberspace’ was one used in science-fiction in the mid-1900s, it came to mean something related (but notably different) during the period of the turn of the millennium. BusinessDictionary.com offers a useful definition of ‘cyberspace’ as follows: Cyberspace is an “imaginary, intangible, virtual-reality realm where (in general) computer-communications and simulations and (in particular) Internet activity takes place. The electronic equivalent of human psyche (the 'mindspace' where thinking and dreaming occur), cyberspace is the domain where objects are neither physical nor representations of the physical world, but are made up entirely of data manipulation and information”

(BusinessDictionary.com n.d.). Cyberspacelaw.org more concisely states that cyberspace "has come to mean the information spaces created by the technology of digital networked computer systems, most of which ultimately connect with the mother of all networks, the Internet" (Chon n.d.). We can say, then, that cyberspace as we know it today exists because of the Internet, where 'Internet' refers to "a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols" (Oxford 2013). Therefore, in a technical sense, cyberspace is created by the data we create and manipulate. It is our creation. Its landscape is a landscape of our own minds' creation. It is a space that is not bound by geography, time or seasons. It transcends the physical world and can be seen as an extension of our, the cyber-citizens', mind-space. Since we project ourselves onto and into cyberspace, it takes on a particularly social nature.

But just how much data, searchable documents, and cultural artefacts (that can be digitally displayed) are we creating? The Internet hosts vast amounts of data, searchable through the World Wide Web – a feature of the Internet that allows for browsing (TechTerms.com 2013). It seems near impossible to find an answer to 'how much data (or information) is on the Internet (or the World Wide Web)'. Instead, estimations are given about how much data transfers on the Internet within a given time – say a few hours, or a month. Estimations are complex and based on web pages indexed by search engines. For example, it is estimated that on 27 July 2013, the indexed web contained at least 3.91 billion pages (WoldWideWebSize.com 2013). Similar situated (as opposed to comprehensive) statements are made, such as "This year, roughly 1.8 million megabytes of data, such as downloaded movies and emails, are produced by the average office worker. By 2015, it is estimated that this amount will double" (Wang 2013). Another example, albeit from Wikipedia, is: "According to the Digital Britain Report, 494 exabytes of data was transferred across the globe on June 15, 2009" where an Exabyte (EB) size is represented as follows:
1 EB = 1000000000000000000B = 10^{18} bytes = 1000petabytes = 1 billion gigabytes (Wikipedia 2013).

Perhaps it is no wonder that a blogger would make the following comment on the size of the Internet: "The scale of information of the Internet is growing at an incomprehensible rate. Similar to the mystifying size of planets and stars" (Camplejohn n.d.). The website WorldWideWebSize.com updates daily in an effort to keep up with estimated measurements of the growth of the massive expanse that is the Internet.

The social nature of cyberspace

As the Internet grows, according to Schmidt and Cohen (2013: 3-4), "our understanding of nearly every aspect of life will change, from the minutiae of our daily lives to more fundamental questions about identity, relationships and even our security". It is imperative that we, cyber-citizens, consider the social consequences of our use of cyberspace with care. Such considerations should be viewed in the context of the processes of globalisation. Our use of cyberspace is both a child of and a mother to the process of globalisation. Schmidt and Cohen from Google acknowledge this, as is stated eloquently:

> Through the power of technology, age-old obstacles to human interaction, like geography, language and limited information, are falling and a new wave of human creativity and potential is rising. Mass adoption of the Internet is driving one of the most exciting social, cultural and political transformations in history, and unlike earlier periods of change, this time the effects are fully global (Schmidt and Cohen 2013: 3-4).

We now need to consider not only that our use of cyberspace has real social consequences, but that those consequences are global in reach and scale. To illustrate how many people are connected to cyberspace, consider the following estimation:

> By 2025, the majority of the world's population will, in one generation, have gone from having virtually no access to unfiltered information to accessing all of the world's information through a device that fits in the palm of the hand. If the current pace of technological innovation is maintained, most of the projected eight billion people on Earth will be online" (Schmidt and Cohen 2013: 4).

Cyber-citizens already rely, to various degrees, on the Internet for banking transactions, business and social communication, and the buying and selling of goods. The use of the Internet is not something we do on the sideline, but is integrated into our daily lives. Cyberspace and the Internet as we know it now would meet the criteria of what Moor calls the 'power stage' of a technological revolution, which is reached when "the technology is firmly established [and] readily available and can be leveraged by building upon existing technological structures [and] most people in the culture are affected directly or indirectly by it" (Moor 2005: 112). It is seen as the final stage of a technological revolution.

It is particularly in times of revolution and transformation that we should be especially aware of Ethics – whether the nature of such transformation is political or technological, since revolutions shift social power lines and create policy vacuums and have unexpected of unforeseen consequences. With regard to the revolutionary powers of Information and Communication Technologies

(ICTs), we need to be aware of how it effects the creation and flow of cultural content (information) that shape our worlds (both virtually and physically), and be aware of which existing social forms are being reproduced or disrupted, according to Kalintiz-Cope in Isfandyari-Moghaddam (2013: 69). The cultural content flowing through ICTs become trusted sources of information for many and we should question this phenomenon, since "the web is now a, if not the, standard reference source for information for most people" (Moor 2005: 114). If this is the case, we need to consider whether the Internet and the information it provides is reliable and safe.

Policy vacuums

An ungoverned space, such as cyberspace, obviously has less policies in place than well-governed spaces (as in the physical world). Only once this becomes a problem can we acknowledge that we need protective policies. Since there are various social problems being manifest in cyberspace, it seems that we do need policies. Due to the fact there are relatively few such policies in place, some authors have begun to refer to 'policy vacuums'. Moor refers to policy vacuums in relation to technological revolutions, explaining that as such a revolution progresses, "more ethical problems will arise since more people are using more technology which causes more policy vacuums and "conceptual muddles" (Moor 2005: 115-116). This is in line with Moor's Law which states that "[a]s technological revolutions increase their social impact, ethical problems increase" (Moor 2005: 117). It seems that social problems, both novel and imported from pre-Internet society are increasing, intensifying, or simply continuing instead of being rooted out.

The problems we face

The Internet hosts vast amounts of useful, positive information. Unfortunately, we, the cyber-citizens, also need to deal with the problematic hosting or transfer of information – in whichever digital format it is represented. Here are just some of the examples of problem areas on the Internet:

(1) The advocacy of behaviour generally related to psychiatric illness. Consider: Anyone, including a child or a teenager, only has to Google "how to be anorexic" or "how to commit suicide" to find a host of answers[5] at how to be 'effective' at being anorexic or committing suicide (instead of being automatically redirected to find help);

(2) pornography and online child sexual abuse. A perverse person can easily create or find recorded and live streaming forms of such footage (Kiss 2013) and spread it to others through peer-to-peer sharing programs;

(3) privacy and security issues such as cyber-bullying, harassment, Internet stalking, online scams, types of surveillance that can run in stealth mode and are easy to download from the Internet (such as key loggers), data mining, hacking, phishing, identity theft and controversial government surveillance (such as PRISM[6]). We cannot be quite sure when our information is where in cyberspace. At the turn of the decade, Google admitted to collecting some private information (passwords and URLs) sent over wireless networks (Wang 2013). Personal information such as e-mail addresses can be gathered, stored and used without consent. For example, a marketing data and software company called Rapleaf is said to have stored and used 80% of all U.S. e-mail addresses (Wang 2013);

(4) targeted unfair discrimination through new and particularly effective ways to discriminate against 'un-liked' communities or individuals. This is done by deleting information about those communities off the Internet, or blocking their access to the Internet and its services all together (Schmidt and Cohen 2013: 184), which would rob them of the possibility of transcending repressive or oppressing environments;

(5) hate-speech inviting forums that may lead to incitement to violence; and

(6) ill-designed applications that are connected to the Internet that cause harm to life, property or privacy. A clear example of a flawed design process is that of the virtual reality game Pokemon Go[7]. Its multitude of negative implications could have been avoided if developers had considered the ethical and social consequences of their product in the design phase.

These are just some examples of emerging issues, and each of them could and should be discussed and debated at length by academics, organisations and governments alike to grasp and address their complexities, but that is beyond the scope of this particular paper. The general point is that we could have foreseen some of these problems, while others continue to emerge and surprise us.

The problems we have created and perpetuated in cyberspace perhaps illustrates that we, the cyber-citizens, were not morally mature enough to handle the freedom of cyberspace responsibly and to be a self-regulating community with the intention of creating a safe space for humanity. Perhaps, handing us the Internet as an unregulated platform was like walking into a school and giving

each child a box of matches and showing them how to strike a match, without giving them any guidelines of when and where to use it and how to do so responsibly. The result is that some children used the matches to light candles on their birthday cake safely and constructively at home, while others set alight books or playgrounds by accident (without harmful intent), while some chose to try and burn each other's hair or clothes. In cyberspace, some of us use the platform of the Internet for constructive purposes, some fall victim to harm, and some outright cause harm. The metaphor of children playing with the matches and unintentionally causing harm could be likened to someone 'surfing the Net' and stumbling upon online pornography and gambling and then, instead of steering away, becomes addicted, losing money and relationships as a result, while he/she never intended to do harm. In the match-metaphor, the school principal would have to instate rules about whether matches are allowed at school - rules which would apply both to the innocent child who needs to light something to demonstrate a science experiment, and the guilty who tried to burn someone's homework on purpose. If the children fail to respect the rules, they will be punished. Surely, this is not a set-up we want for the use of the Internet, since its specific power comes from exactly the fact that we have a relatively free information platform. The fact is not that all of us, the cyber-citizens, are good citizens, which raises the question whether we do, in fact, need some form of regulation of our online behaviour.

Regulation from three angles: government, ICT design and information ethics

Regulation by government and/or internet service providers

Eric Schmidt (Executive Chairman of Google) and Jared Cohen (Director of Google Ideas) have stated that the Internet is "the largest experiment involving anarchy in history" (Schmidt and Cohen 2013: 3). It could be argued that this experiment has proven both effective in stimulating innovation, and allowing the abuse of freedom. The regulation of the Internet, cyberspace, and the flow of digital communications and media is an extremely tricky area – effectively a tightrope of balancing of interests. Governments can misuse power in this sense to discriminate against groups, cripple social mobilisation efforts or cut off fair information supply from its citizens.

In South Africa some initiatives have been taken in the form of, for example, RICA – the Regulation of Interception of Communications and Provision of Communication-related information Act, 2002[8] and the Protection of Personal Information Bill[9]. China has a much debated "policy of active censorship, where censors automatically shut down the connection whenever a prohibited word is

sighted" (Schmidt and Cohen 2013: 184). The then Prime Minister, David Cameron of the United Kingdom in 2013 called for international collaboration to root out online child sexual abuse (child pornography) stating that "[t]here is a triangle. We have to stop the people putting up the images, stop those accessing it and ask internet companies to do better in stopping them to access it" (Kiss 2013). Any government regulation will have to be in collaboration with internet service providers (ISPs). This idea will be challenged by advocates of network neutrality[10]. Even where network neutrality is an issue, some authors seem to gloss over areas such as online sexual abuse in a passive acceptance of the need to filter out certain content on moral and legal grounds, as is seen in an extract from a conference paper by Craig McTaggart titled *Was the Internet Ever Neutral?* which reads as follows:

> While rarely controversial, ISPs routinely filter and block certain traffic – based on source address, port number, and/or payload profile, for example – in order to stop the egress and ingress of abusive and malicious Internet traffic such as spam, viruses, and network-based attacks. This fact alone contradicts claims that all Internet content and traffic is equal, though net neutrality advocates often allow for this kind of ISP intervention under the umbrella of 'reasonable network management' (McTaggart 2006: 9).

If ISPs are willing to put protective measures in place for computer security and safety, then perhaps they can partner with governments, Non-Government Organisations, Community Based Organisations and wider stakeholder groups to put measures in place to protect human security and safety. Regulation through the design of new ICTs is another form of regulation which might take some of the burden off governments, although this may also take place in collaboration with governments[11].

Regulation through design

Cameras on mobile phones were obviously designed to take photographs and videos. We can take and share these photographs and videos of our holidays, weddings and parties. We can also use them in ways that impose on human privacy or dignity, for instance by taking photographs in gym dressing rooms of unwitting people and posting these photographs on public platforms. Surely the designers of the technology do not design ICTs for the purpose of abuse, yet once in human hands, it is the very capabilities of these devices that allows for the abuse. Other technologies that operate in the background of cyberspace are less obvious than a digital camera and include forms of Computational Intelligence. These can be employed in useful ways, for example in the case of Artificial Neural Networks that can both structure online libraries, such as the Fast Artificial Neural Network Library[12] (the FANN library) or be used as state of the art tools in digital forensics; or alternatively for more sinister projects

such as data mining and the surveillance of online behaviour. In order to proactively prevent abuses, at least three design approaches have been proposed, namely (1) Anticipatory Technology Ethics, (2) Values-sensitive design, and (3) the programming of Artificial Moral Agents.

Anticipatory Technology Ethics

The need for better design has been acknowledged by some authors. Consider the following quote: "[d]esigning for (moral and non-moral) values has become increasingly important for technology development in recent years" (Pommeranz, Detweiler, Wiggers and Jonker 2012: 285). Moor has also called for "better ethics for emerging technologies" (Moor 2005: 111). Phillip E.A. Brey (2012) responds to Moor's call for better ethics for emerging technologies by proposing a model for anticipating ethical issues through Anticipatory Technology Ethics. Brey (2012: 305) proposes a technique of ethical analysis that aims to anticipate the ethical issues that might arise from the creation or application of emerging information technologies, an approach that he calls 'anticipatory technology ethics' (ATE). He defines 'emerging technologies' as "technology at the R&D[13] and introduction stages" of the development of technology (Brey 2012: 306). He argues that "[u]ltimately, ethical assessment of emerging technologies concerns the question of what is good and bad about the devices and processes that they may bring forth, and what is right and wrong about ways in which they may be used" (Brey 2012: 306). The argument is made that, despite the obvious problem of dealing with uncertainty in emerging technologies, dealing with ethical issues only once technologies are fully developed and the social impacts have become clear is costly and that by this time it is "more difficult to steer technology development into a more ethical direction" (Brey 2012: 307). He proposes that designers and developers should start taking ethical issues into account as early in the process as at the R&D phase.

Value Sensitive Design

Another attempt to reconcile ethical values and technology is also based on locating responsibility for "considering human values in the design process of socio-technical systems" (Pommeranz, Detweiler, Wiggers and Jonker 2012: 285) with the designers. Pommeranz et al. (2012) explain the aspects of Value Sensitive Design, as proposed by Friedman, Kahn and Borning. The aim of the Friedman, Kahn and Borning (2006) Value Sensitive Design (VSD) framework is to take human values into account in the design process of technology (Pommeranz, Detweiler, Wiggers and Jonker 2012: 290). The VSD framework consists of three integrated investigations, namely (1) a conceptual investigation

which is aimed at discovering and analysing values and value tensions as well as the identification of stakeholders; (2) an empirical investigation of the context in which the technology is used; and (3) a technical investigation focused on the technology itself and how it caters for or opposes human values (Pommeranz, Detweiler, Wiggers and Jonker 2012: 285-290). The designers of technology which has social impact are partly responsible for taking human, ethical values into account during all stages of developing a new technology and the VSD framework provides practical guidelines for this design process (Pommeranz, Detweiler, Wiggers and Jonker 2012: 285-286). It is not however clear whether this approach is used in practice or not.

Pommeranz, Detweiler, Wiggers and Jonker (2012) point out that the application of VSD might be problematic. Potential problems may include "missing some values of importance, e.g. due to a strong focus on the values identified by the designer in conceptual investigations, lack of stakeholders' ability to envision new technology and its influence on their values, or misinterpretation/-communication between designers or stakeholders" (Pommeranz, Detweiler, Wiggers and Jonker 2012: 286). They respond to these potential problems by proposing a model for eliciting situated values. Their tool is certainly worth more attention than can be afforded to it in the scope of this paper.

Artificial moral agents

A third approach, dealing directly with artificially intelligent technologies is discussed by Allen, Smit, and Wallach (2005) where top-down, bottom-up and hybrid approaches to creating artificial morality is discussed. Artificial morality saves the ignorant/innocent end user of intelligent technologies from being 'delivered' to technologies which they do not fully understand due to the fact that "artificial morality shifts some of the burden for ethical behaviour away from designers and users, and onto the computer systems themselves" (Allen, Smit, and Wallach 2005: 149). This is an approach of creating artificial moral agents and currently in an experimental stage, and is problematised by various philosophical theories.

Challenges to these approaches

All three approaches, namely Value Sensitive Design, Anticipatory Technology Ethics and the creation of Artificial Moral Agents pose definite problems. All three approaches face the same problem of viability, namely that of interdisciplinary dissonance, as all three approaches require a multi-disciplinary approach. With regard to the latter, Moor (2005: 118) rightly says that "people who both understand the technologies and are knowledgeable about ethics are in

short supply just as the need is expanding". Furthermore, each model has problems of its own. Anticipating ethical problems relies on futures studies which are uncertain and provides only vague glimpses into the future. VSD requires time for stakeholder engagement, and time is of the essence to compete successfully in the ICT world. The creation of Artificial Moral Agents currently raises more questions than answers and is still some way from becoming a viable option.

Addressing the problem

Governance of cyberspace will fall on governments. Governments will have to carefully navigate between the protection of human rights where human rights are in conflict with each other, such as the right to dignity versus the right to free speech. Governments will have two broad options: (1) a top-down approach which would enforce laws affecting ISPs, designers of ICTs, search engines and users. This could be particularly problematic in countries ruled by oppressive regimes. It would also not contribute to the moral maturity of its citizens; or (2) a diffusion approach through which government/s engage in initiatives to instigate and fund information ethics awareness campaigns. These campaigns would give citizens the opportunity to mature morally and make better decisions by themselves in terms of their consumption and generation of online content. I would strongly recommend the diffusion approach.

The South African government is already setting an example in this regard, in that it has launched a co-operative process between the national Department of Communications and the University of Pretoria through the African Centre of Excellence for Information Ethics (ACEIE). This process enables the staff of the ACEIE to present information ethics workshops in various provinces in South Africa (as well as in other African countries) in order to gain an understanding of African information ethics. The ACEIE is linked to the African Network for Information Ethics[14] (ANIE) which led the way in the adoption of the 2007 Tshwane Declaration of Information Ethics in Africa which advocates that "[i]nternational academics and policy makers should enhance African dialogue on developing norms and values for the African information society" (South Africa: Conference adopts … 2007). This co-operation indicates that the South African government may be aiming towards a diffusion approach where ethics and the freedom it grants takes precedence over laws and their restrictive nature.

The role of information ethics as an alternative to regulation approaches (very briefly)

Information ethics is a branch of applied ethics. Information ethics deals with the problems highlighted in point 2 of this paper, as well as with copyright and plagiarism issues and other matters. Due to the fact that information ethics is applied ethics, we need to keep in mind that it is a "dynamic enterprise that continually requires reassessment of the situation" (Moor 2005: 118).

Information ethics as a field is in its infancy and a lot of future work is still to be done. Since we, the cyber-citizens, have not proven ourselves to be good stewards of our collective freedom in cyberspace, we clearly need information ethics, not in an exclusively prescriptive, or descriptive form, but in an applied form that aims towards the ethical sensitisation of cyber-citizens. The aim of information ethics cannot be to create or enforce rules, but instead it should be to cultivate virtuous cyber-citizens through knowledge and awareness that can put them on the way to the journey of moral maturity. I propose ethical sensitisation on the following levels:

(1) Ethics sensitisation through training and education for and by the gatekeepers of information: internet service providers, search engines, educators and parents.

(2) Ethics sensitisation through training and education for the user of the Internet that consumes information and generates content (called User Generated Content – UGC).

(3) Ethics sensitisation for and by national governments and international co-operation through training and education. This means that governments cannot follow a strict top-down approach, but should engage with multiple stakeholders to find out what their needs and views are – especially in the African context.

For the effective advancement of information ethics and better ethics for emerging technologies, Moor suggests that three things are needed, namely (1) acknowledging that ethics is an "ongoing enterprise"; (2) to "establish better collaborations among ethicists, scientists, and technologists"; and (3) "to develop more sophisticated ethical analysis" (Moor 2005: 118). Moor also points out that "[b]etter ethical thinking in terms of being better informed and better ethical action in terms of being more proactive are required" (Moor 2005: 111). It is the duty of every cyber-citizen to contribute to the creation of an online world that is safe, shows respect to both human dignity and freedom, and protects vulnerable cyber-citizens such as children and those who lack information-literacy. If we as cyber-citizens take up this role, we will not need

to be forcibly regulated by government interventions. If, however, we do not recognise that we form a globally interconnected community that needs to be self-regulating in our management of information, we may need government regulation after all. In recognising the threat that governments can abuse such powers, we need to become pro-actively involved in creating information ethics awareness, so that we, the cyber-citizens, will be allowed to enjoy the freedom granted by the Internet responsibly, and sustainably.

Conclusion

Cyberspace is largely ungoverned, and as cyber-citizens we have allowed the perpetuation and creation of social problems. This can be addressed by government regulation, ICT design methods that are ethically sensitive, or by creating information ethics awareness. Where governments intervene, power can be abused. It may be a morally responsible move for the designers of ICTs to take ethical considerations into account at various stages of the design process. Ultimately, new challenges will keep arising with every technological revolution which includes the adoption of new ICTs. A more sustainable approach for protecting cyber-citizens from falling victim to or creating new social problems via cyberspace is sensitisation to and the creation of awareness about information ethics through training and education. A three-pronged approach which includes governments, designers and the promotion of ethical awareness (especially information ethics) might be needed. The challenge, and a necessary topic for further investigation, is how these three should be balanced to achieve a safe and free virtual world, inhabited by good (responsible and morally mature) cyber-citizens.

References

Allen, C., Smit, I. and Wallach, W. 2005. Artificial morality: Top-down, bottom up, and hybrid approaches. *Ethics and information technology* 7: 149-155.

Brey, A. E. 2012. Anticipating ethical issues in emerging IT. *Ethics and information technology* 14: 305-317.

BusinessDictionary.com. n.d. Cyberspace. *BusinessDictionary.com*. http://www.businessdictionary.com/definition/cyberspace.html Accessed 23 July 2013.

Camplejohn, D. n.d. How much data is on the Internet? *Fliptop blog* http://blog.fliptop.com/blog/2011/05/18/how-much-data-is-on-the-internet/ Accessed 27 July 2013.

Chon, M. n.d. Introduction to cyberspace and law: the relation of law to cyberspace and of cyberspace to law. *Learning cyberlaw in cyberspace*. http://www.cyberspacelaw.org/chon/ Accessed 27 July 2013.

Friedman, B., Kahn, P., and Borning, A. 2006. Value sensitive design and information systems. In *Human-computer interaction and management information systems: foundations*. New York: Sharp, pp.348-372.

Horner, D. S. 2005. Anticipating ethical challenges: is there a coming era of nanotechnology? *Ethics and information technology* 7: 127-138.

Isfandyari-Moghaddam, A. 2013. Book Review: Rocci Luppicini: Ethical impact of technological advancements and applications in society IGI Global, Hershey, PA, 2012, 357 p. *Ethics and information technology* 15: 69-71.

Kiss, J. 2013, July 22. UK government to 'drain the market' of online child sex abuse. *The Guardian*. http://www.guardian.co.uk/technology/2013/jul/22/uk-government-online-child-sex-abuse Accessed 27 July 2013.

McTaggart, C. 2006. Was the internet ever neutral? *Prepared for the 34th Research Conference on Communication, Information and Internet Policy*. George Mason University School of Law, Virginia, U.S.A. http://www2.le.ac.uk/departments/media/dl/documents-and-pdfs/course-readers/penm/WastheInternet.pdf Accessed 26 July 2013.

Moor, J. H. 2005. Why we need better ethics for emerging technologies. *Ethics and information technology* 7: 111-119.

Oxford. 2013. Definition of Internet in English. *Oxford dictionaries*. http://oxforddictionaries.com/definition/english/Internet Accessed 27 July 2013.

Pommeranz, A., Detweiler, C., Wiggers, P. and Jonker, C. 2012. Elicitation of situated values: need for tools to help stakeholders and designers to reflect and communicate. *Ethics and information technology* 14: 285-303.

Schmidt, E. and Cohen, J. 2013. *The new digital age: reshaping the future of people, nations and business.* London: John Murray.

South Africa: Conference adopts Tshwane Declaration on Information Ethics. 2007. http://allafrica.com/stories/200702080355.html Accessed 14 July 2015.

TechTerms.com. 2013. Internet. *TechTerms.com*. http://www.techterms.com/definition/internet Accessed 27 July 2013.

Wang, A. 2013. Infographic: how much of your data is on the net? *SecurityWatch with Neil Rubenking*. http://securitywatch.pcmag.com/security/313683-infographic-how-much-of-your-data-is-on-the-net Accessed 25 July 2013.

West, D. 1996. *An introduction to continental philosophy.* Cambridge: Polity Press.

Wikipedia. 2013. Exabyte. *Wikipedia the free Encyclopedia*. http://en.wikipedia.org/wiki/Exabyte Accessed 27 July 2013.

WoldWideWebSize.com. 2013. The size of the wold wide web (The Internet). *WoldWideWebSize.com - Daily estimated size of the World Wide Web*. http://www.worldwidewebsize.com/ Accessed 27 July 2013.

Endnotes

[1] For the purpose of this paper 'cyber-citizens' will refer to all of us who use the Internet – that is those of who can use it because we have the necessary literacy to do so, as well as access to the hardware, software, electricity and connectivity to do so. Those who do not have this type of access should not be excluded from research and debates, but it will fall under the topic of the Digital Divide. Though the Digital Divide is a very important topic in information ethics, it will not be dealt with in the scope of this specific paper.

[2] Although one's physical environment may prohibit one's access to cyberspace if there is no connectivity etc. available. Again, this is for discussion under the topic of the Digital Divide.

[3] "Great" relative to the freedoms we have elsewhere – not a 'complete' freedom, since we are still bound by the modes of signification (through signifiers) by way of format and transfer according to the programs we use.

[4] For example: The case of the "Arab Spring".

[5] Examples of websites: http://whyeat.net/forum/threads/31330-Anorexia-to-bulimia and http://lostallhope.com/suicide-methods/statistics-most-lethal-methods. WARNING: Some of these types of sites contain malware like Trojan Horses!

[6] "PRISM is a clandestine mass electronic surveillance data mining program operated by the United States National Security Agency (NSA) since 2007" http://en.wikipedia.org/wiki/PRISM_(surveillance_program), Accessed 26 July 2013.

[7] The mass uptake of Pokemon Go has had serious consequences for players and communities, such as robberies (https://www.rt.com/uk/350814-pokemon-game-warnings-crime/), using public spaces inappropriately (https://www.rt.com/viral/350863-holocaust-museum-pokemon-go-stops/), ignoring serious injury (http://m.fin24.com/fin24/Tech/Mobile/pokemon-go-digital-popularity-is-also-warping-real-life-20160713), causing motor car accidents (http://m.wheels24.co.za/wheels24/News/you-dont-gotta-catch-em-all-pokemon-go-sends-driver-crashing-20160714), and even a situation where a player crossed a highway for the sake of the game) http://www.stltoday.com/news/national/pokemon-players-are-trespassing-risking-arrest-or-worse/article_be7d440f-c2a5-54cb-9a29-ae56ba7208cc.html). These behaviours could have been anticipated and design adjustments could have been made, such as plotting certain areas (such as highways and train stations) as off-limits in the game. All web addresses accessed 14 July 2016.

[8] http://www.info.gov.za/gazette/acts/2002/a70-02.pdf

[9] http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionofPersonalInformation.pdf

[10] A state where all Internet content and traffic are treated equally (McTaggart, 2006).

[11] This could be a very dangerous step though – if government interferes to the point where it hampers innovation or a healthy measure of social and industrial freedom.

[12] http://leenissen.dk/fann/wp/

[13] Research and Development.

[14] http://www.africainfoethics.org/index.html