Concepts in Information Ethics

An introductory workbook

Editors: Candice le Sueur, Erin Hommes and Coetzee Bester

Concepts in Information Ethics:

An introductory workbook

2013

ISBN 978-1-920527-84-6

Editors
Ms Candice le Sueur
Ms Erin Hommes
Mr Coetzee Bester

Production
Hercules Boshoff
Rachel Bothma
Erin Hommes
Candice le Sueur

Published By
African Centre of Excellence for Information Ethics
Department of Information Science
University of Pretoria
South Africa

Printed By
Groep 7 Drukkers & Uitgewers BK (1993/24129/23)
Posbus 14717, Sinoville, 0129
Tambotieweg 776, Kameeldrif-oos, Pretoria
GPS: Suid 25° 37' 35.2" Oos 28° 17' 51.8"

Contents

Foreword

Since the first African Conference on Information Ethics was held in February 2007, various academic institutions, government departments and private sector stakeholders have contributed to the expansion of the work and objectives set by the conference. These objectives not only included the growth of an awareness of Information Ethics in Africa but also to formally research the topic and to teach the new knowledge in formal courses at universities.

As signed on the 15th of December 2011, the Memorandum of Agreement between the University of Pretoria and the Department of Communications signalled the official start of the African Centre of Excellence for Information Ethics' (ACEIE) activities. The ACEIE endeavours to be a hub for research and of networks between all parties passionate about and interested in Information Ethics in Africa.

In support of the mentioned academic objectives, the Africa Network for Information Ethics (ANIE) and the ACEIE were structured to further support the UNESCO activities in WSIS on the African continent.

The ACEIE coordinates research and academic activities to enhance the awareness and knowledge of all stakeholders and role players on the matter of Information Ethics. The activities include workshops, conferences and public lectures, as well as books and articles.

The ACEIE activity of coordinating workshops in Africa means that more individuals will become connected with this network and allow them to do their own research on the topic. The compilation of books and writing of articles will ensure that research remains current and thought-provoking and that the efforts of both the ANIE and ACEIE result in a positive impact on society.

This workbook, "Concepts in Information Ethics", contributes towards this undertaking of the ACEIE. The *Concepts* aims to equip researchers, scholars, government officials, non-government organisations and community-based organisations with Information Ethics vocabulary. This vocabulary entails descriptive paragraphs, together with a one sentence definition encapsulating the core meaning of a concept. Following on these definitions, ample space is provided for the user to make notes or add relevant examples to further enable their understanding of the concept.

The Concepts in Information Ethics workbook is therefore a working document aiming to provide a platform for understanding in Information Ethics as well as a point of departure for academic discussion.

I would like to thank the editors and production team for their dedication and hard work in compiling this volume, as well as the following people for their on-going support and dedicated initiative to further develop Information Ethics in Africa, they are: Prof Johannes Britz, Prof Rafael Capurro, Prof Stephen Mutula, Prof Dennis Ocholla.

I trust that the reader will find this workbook as inspiring as those who recognised the need to compile it.

Professor Theo Bothma

ACEIE Management Committee and HoD of Information Science

University of Pretoria, September 2013

About this book

The aim of this workbook is to create a user-friendly reference for use in various contexts and on different levels. We have therefore compiled this workbook with simplified definitions/descriptions of some of the concepts used in discussions pertaining to Information Ethics. The aim of this workbook is to equip readers with some of the necessary vocabulary to effectively engage in such discussions. This workbook is in no way intended as an academic treatise that discusses the concepts in their comprehensive depth and breadth. We have also decided to use "you", "we", "yours" etc. instead of "subject", "agent", etc. in the spirit of creating an introductory text that is easy to use beyond the academic sphere.

Facilitators using this book are encouraged to:

- *Start by introducing the two main concepts: "Ethics" and "Information Ethics" – always reading "Information Ethics" in conjunction with "Ethics".*
- Use the concepts specifically as a starting point for open discussion, rather than an end point.
- Provide and get every-day examples from participants to contextualise the concepts.
- Encourage readers/participants to take notes in the open pages that are specifically allocated for this purpose next to every concept.
- Let readers/participants know that they are free to question and contest the content we have generated in order to stimulate critical thinking.
- Help readers/participants to understand how these concepts are relevant in their every-day lives and what their own rights and responsibilities are.
- Point out that the e-mail address for the African Centre of Excellence for Information Ethics is on the back cover, and that we would welcome their feedback.

We have distributed this workbook in draft form at some of our workshops this year and it has been welcomed with much enthusiasm. We hope that you will find it useful too.

Candice le Sueur

ACEIE Junior Research Officer

University of Pretoria, September 2013

Acronyms

ACEIE	African Centre of Excellence for Information Ethics
COMNET-IT	Commonwealth Network of Information Technology for Development Foundation
CSR	Corporate social responsibility
ICT	Information and Communication Technology
IE	Information Ethics
OECD	Organisation for Economic Co-operation and Development
UN	United Nations
PDA	Personal Digital Assistant
UGC	User-Generated Content
UNESCO	United Nations Educational, Scientific and Cultural Organisation
WSIS	World Summit on Information Society

CONCEPTS IN INFORMATION ETHICS

1. Access to information

It refers to the means (like a mobile or other computing device; or transport), processes (like needing an ID to register for a library card), or rights (like privacy bills) related to obtaining or providing information.

Access to information is promoted by the development of new ICTs that provide remote access to information. It is a combination of physical, intellectual and social elements that have an impact on information availability to individuals (www.education.com, 2013; Jaeger & Burnett, 2005).

Access of information is hindered by laws, censorship, and some archiving processes. A significant hindrance to access information is the cost of information that is not affordable to would-be users of the information.

Image: office.microsoft.com

Promotion of Access to Information Act No 2 of 2000 (a.k.a. PAIA)

The Promotion of Access to Information Act No. 2 of 2000 (as amended by the Promotion of Access to Information Act No. 54 of 2002) gives effect to the constitutional right of access to information held by the state and information held by any other person that may be required for the exercise or protection of any rights.

Without free access to documents published by either the government or private citizens in a country, freedom of information is limited and incomplete. The Act represents a significant characteristic of democracy namely empowering the people by providing them with a statutory mechanism to be used in order to access crucial information.

2. Accessibility of information

"Information accessibility encompasses many issues surrounding availability, accessibility and affordability of information" (UNESCO, 2013).

Accessibility in information systems is important for avoiding discrimination. Accessibility should encompass all access related issues, including "multilingualism, metadata, interoperability, open source software, open content, Creative Commons licences as well as addressing the special needs of people with disabilities" (UNESCO, 2013). In some countries, the presence of a Disability Discrimination Act makes it a legal requirement for websites to be usable regardless of disability.

The more accessible information is the more people can make use of it. A user-unfriendly or inaccessible website, for instance, can restrict or remove access from a significant proportion of users.

Safe access to information vs. Access to safe information

In the current information age, the magnitude of access to information on the internet raises some unique safety concerns. Users of internet services need the reassurance that they are offered safe access to information, through security safeguards. This is particularly relevant in financial services, where internet banking and electronic wallets are becoming the preferred methods of monetary exchange (WWWMetrics, n.d.). Without these safeguards, users run the risk of becoming victims of cybercrimes such as identity theft/fraud or phishing.

In addition, the importance of access to safe information can be seen in the use of various forms of content control, particularly on the internet. Governments, legal authorities and influential online companies such as Google all emphasise the importance of protecting internet users, particularly those below the age of 18, from harmful and immoral content. Content control and filtering services such as NetNanny (www.netnanny.com) and parental controls available on satellite television services are all tools to ensure that younger viewers access only safe information.

3. Accountability

The ability and responsibility of an individual to give account to some other party for their actions – for instance a state of being liable or answerable for the integrity of information they deal with (Investopedia, 2013).

Everyone who is in a position of power or trust is accountable to the persons who give them that power or trust by electing or employing them. In this way, citizens have the responsibility to hold government accountable for what it does. Government has to answer for its actions towards the citizens it serves. The same goes for other public, private and voluntary organisations where officials have to answer to someone for their actions and take responsibility for them (Business Dictionary 2013; T/A Initiative, 2013).

Image: savagechickens.com

4. Censorship

Limiting the type and content of information made available to the public by removing what is deemed to be immoral or not in the best interest of the recipients of the information.

Censorship refers to the official supervision and control of information, ideas, or artistic expression by anyone, circulated among the people within a society, which is considered a threat to political, social or moral order.

Contemporary definitions of censorship refer to the examination of books, periodicals, plays, films, television and radio programs, news reports, and other communication media for the purpose of altering or suppressing parts of thought to be objectionable or offensive.

It may be imposed by local or national government authority, by a religious body, or occasionally by a powerful private group or speakers, writers, and artists themselves (Bram & Dickey, 1993; Grolier Inc., 1997; Lagasse, 2001).

There are a number of criticisms against censorship. These include how censorship undermines society's ability to use its own discretion; its ability to hinder political opposition; that it ends up drawing more attention instead of deflecting it; and that censorship is a threat to freedom of expression.

Internet Censorship

"The Open Network Initiative reports that nearly 60 countries around the world restrict Internet communications in some way, and it is likely that far more entities manipulate content or communications in some fashion…. Organizations or countries may restrict access to information using techniques that range from blocking communications entirely, to degrading performance (sometimes to the point where a service might be unusable) to manipulating content to spread misinformation" (Burnett & Feamster, 2013).

Image: http://schoolriff.wordpress.com

5. Cloud computing

Using networked software and applications offered over the Internet rather than on a personal device.

To introduce the concept of cloud computing, Ann Cavoukin's (2008) descriptions of the Cloud and Cloud Computing will be used:

The Cloud

- That unpredictable part of an electronic network through which data (including personal information) passes from one end to another, being processed and stored along the way.
- It is comprised of a networked collection of servers, storage systems and devices that combine software, data and computing power otherwise scattered in multiple locations across the network.
- It is controlled by third parties and individuals have little direct knowledge, involvement or control over it.
- It stores information everywhere except on personal computing devices.

What does this mean for Cloud Computing?

- Internet users can access programs and databases on the Internet as a service, and access and share information without storing major software on their personal devices, since the data and software reside on the internet. Data can also be saved in the cloud where it is safe from personal device hardware malfunctions.
- Users do not need expertise or knowledge about the functioning of the cloud to use it, and neither do they need (or in general have) control over the technological infrastructure that supports 'in the cloud' operations.

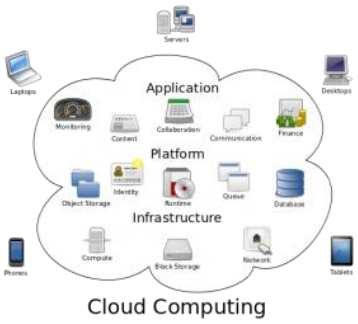
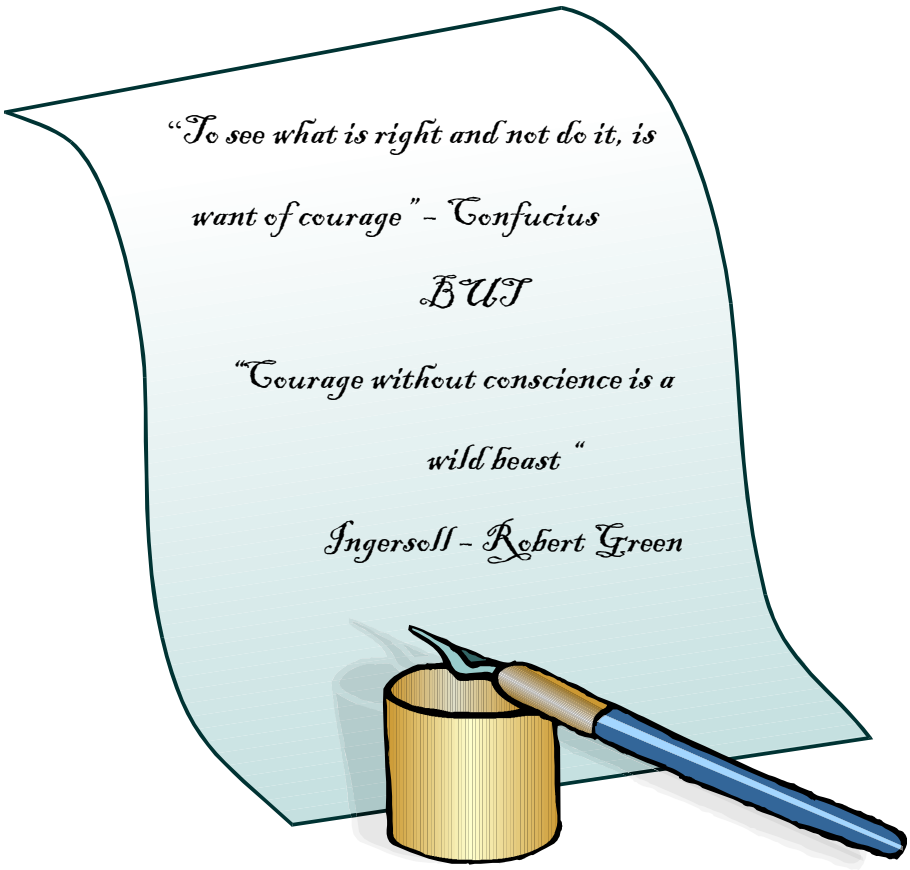


Image: fossforce.com

6. Conscience

An awareness of the difference between right and wrong that guides individuals towards doing what is right.

Your conscience is a part of the psychological make-up of humans that enables us to differentiate between right and wrong, or good and evil. It makes us aware of it that something is morally forbidden. It causes us to feel guilt and remorse when we do what we believe is wrong. It guides us towards doing what we believe to be good and right. Our conscience is guided by our religious or moral beliefs/convictions. It develops and grows stronger as our beliefs/convictions grow stronger. Our conscience tempers other values that could be misguided, like courage, loyalty and determination. For example, your conscience might make you aware that something is 'not right' when you are loyal to a group or movement that violates the basic rights of others.

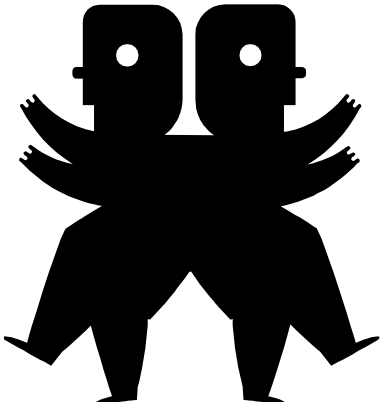


7. Conflict of interest

Typically, a conflict of interest arises when someone in a position of trust acts, or executes their job, in a self-interested way that conflicts with the interests of their firm.

Even when a person in a position of trust is not acting in a decidedly self-interested manner, a conflict of interest can occur. When a person has more than one interest, their decision-making with regards to any one of these inter-related interests cannot be considered to be objective or unbiased.

These interests are substantial enough that is affects the employee's independent judgement when making decisions on the employer's behalf. Some conflicts of interest can turn into moral dilemmas.



Write down an example of a 'conflict of interest' situation that you have been in, or that someone has shared in the workshop:
Which interests were in conflict with each other?
Why were those interests in conflict with each other?
How did you/the person end up in that situation?
How did you/the person handle the situation?
What were the consequences?

8. Corporate Social Responsibility (CSR)

The ethical responsibility that corporations have towards the society they operate in.

Consider the enormous social and economic impact that ICT corporations and platforms, like Microsoft, Apple, Google, Facebook, Blackberry, Twitter, Nokia, MTN etc. have on an international scale. Their products and services determine how we communicate, format, and disseminate information. If these ICT giants focus purely on profits without taking responsibility for their impact on society, serious harm could be done to social order.

Considering the consequences of our actions is a necessary part of being a good citizen. Although corporations are not persons, they are legal entities with legal rights and responsibilities. On these grounds it may be expected that corporations behave like good citizens, by aligning their behaviours with the societal norms, values, objectives and expectations (Carroll, 1999; Kohonen, 2003).

To this effect, corporations are sometimes expected to:

- Take responsibility for and solve social problems they cause or contribute to
- Allocate resources to broad social ends, like helping other major institutions (like governments and universities) to achieve social progress
- See to it that production and distribution of their products contribute to overall socio-economic welfare. This point is important to consider alongside the issue of information poverty.

Corporations are increasingly expected to take responsibility for their effects in three domains: Social, Economic, and Environment. Ideally, an organisation's responsibility towards society should increase to the degree that the organisation's impact on society increases.

Image: office.microsoft.com

9. Corruption

Corruption takes place when dishonest acts are rewarded.

It is the act of corrupting or being corrupt. When someone is being corrupt, it means that they are willing to act dishonestly in return for money, personal gain or an unfair advantage. Corruption therefore always involves some form of exchange.

A transaction or exchange is seen as being corrupt:

a. When it serves the interest of a third party or is linked to an abuse of authority
b. When someone accepts illegitimate benefits (known as 'passive corruption')
c. When someone offers illegitimate benefits (known as 'active corruption')

Corruption undermines the functioning of governmental, legal and social processes and stability, and hampers trust in persons in positions of authority.

Discuss: Which new forms can corruption take in the *Information Age*?

Image: office.microsoft.com

10. Cyber-bullying

Bullying that takes place online, or through the use of mobile devices.

Cyber-bullying takes place when children and teenagers wilfully use technology (like computers, the Internet, mobile phones etc.) to repeatedly inflict harm (Cyberbullying Research Centre, 2013) on another child or teenager by harassing, humiliating or threatening them (Nemours, 2013).

When the harassment is not between two minors and adults become involved, it is no longer called cyber-bullying, but is referred to as cyber-harassment or cyber-stalking instead (Stopcyberbullying.org, n.d.).

The new Protection from Harassment Act in South Africa 2013

Extracts from ITWeb Security news report (Mawson, 2013):

In terms of the Protection from Harassment Act, someone who has been bullied can ask the courts for an interim protection order, which will be granted as long as the court is satisfied the respondent has harassed, or is harassing, the applicant and that harm has or may be caused.

In order to track down offenders who bully behind the cyber wall, the Act stipulates that electronic service providers can be forced to hand over the name, surname, identity number and address of the person to whom the IP address, e-mail or cell phone number belongs.

As soon as the order is made final, the applicant will also receive a warrant of arrest that can be handed to the police if the bully fails to abide with the order. Any person who contravenes the order can be jailed for as long as five years.

In addition, if electronic communications service providers, or their staff, fail to hand over information, they can be fined R10 000, while staff can be jailed for six months.

Source: http://www.itweb.co.za/index.php?option=com_content&view=article&id=63654

11. Cyber-citizen

The term "cybercitizen" denotes a "citizen of the Internet" or a member of the "cybercommunity" (Rouse, 2005).

A good citizen of a nation has certain roles and responsibilities, like obeying laws and holding government responsible for their actions. In cyber-space, users of online services and platforms also have certain duties and obligations.

Here are ten ways recommended to be a good cyber-citizen (Wizbowski, n.d.):

1. Protect your digital identity
2. Use a personal security device when going online
3. Use antivirus and antispyware software
4. Teach family and friends about the importance of strong passwords
5. Get involved in your child's online life
6. Report cyber-crimes (like phishing)
7. Protect your home or small business Wi-Fi network from others gaining access to it (which could allow them to 'eavesdrop' on what you are doing online), by implementing the authentication security capabilities built into your Wi-Fi adaptor.
8. If you are a parent, consider parental control systems for Internet access on 3G mobile phones
9. If your bank does not provide a smart bankcard, know the other safe ways to shop online
10. Do not share information with web sites you don't trust

Furthermore, it would be safe to say that a good cyber-citizen will not intentionally harm any other member of a cyber-community; will not commit cyber-crimes; and will apply his/her moral principles both in offline and online environments.

Image: research.cc.gatech.edu

12. Cyber-crime

Cyber-crime refers to criminal offences committed in cyberspace using computers and the Internet.

Cybercrime.org.za provides the following definition: "Cybercrime is generally defined as any form of criminal activity involving the use of computers and networks. It is also referred to as computer crime, electronic crime, e-crime, netcrime and hi-tech crime" (http://cybercrime.org.za/, 2013).

According to Interpol, it is one of the most rapidly growing areas of crime, and includes: Attacks against computer and data systems; identity theft; the distribution of child sexual abuse images; Internet auction fraud; the penetration of online financial services; and the deployment of viruses, Botnets, and various email scams such as phishing (INTERPOL, 2013). According to the US FBI, it additionally includes cyber-based terrorism and espionage (FBI.gov, n.d.).

In cyber-crime situations, computers can be used as weapons (as a means of committing the crime), a target (of viruses for example), or an accessory to a crime (storing illegally gotten information) (Cybercitizenship.org, n.d.).

To avoid becoming a victim of Internet banking fraud or cell phone banking fraud (two prominent cybercrimes), Clive Pillay, the South African Ombudsman recommends the following (Coetzer P. , 2013):

Never click on a link in an email that purports to come from a bank.

Never respond to an apparent internet banking related email.

Never provide any information of your online banking details in response to a phone call.

13. Cyber-warfare

Cyber-warfare is a politically motivated form of information-warfare. It refers to attacks in cyberspace that could threaten the security of a nation, or its ability to provide essential services to its citizens.

If warfare refers to attack-and-retaliation strategies governed by international laws of war, then cyber-warfare is a reality (Coetzer, 2013). Cyber-attacks are sometimes seen as acts of sabotage, terrorism, 'use of force', or understood as a 'data war'. US intelligence regards cyber-attacks as one of the largest threats to their national security (Coetzer, 2013).

A cyber-attack can be defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (Broucek & Turner, 2013). This definition can be enhanced by the one provided in the Tallin Manual used by Nato (North Atlantic Treaty Organisation) which states that cyber-attacks are "reasonably expected to cause injury or death to persons or damage or destruction to objects" (Coetzer, 2013).

Cyber-attacks use malware (malicious software) to exploit organisational vulnerabilities (Broucek & Turner, 2013). One type of attack is called a Denial of Service (DOS) attack, which harms an organisation's online presence and e-commerce facilities, effectively bringing operations to a halt (Broucek & Turner, 2013). Critical infrastructure like power-grids can also be subject to cyber-attacks.

Image: scientificamerican.com

14. Deontological Ethics

It is a theory of ethics that proposes a universal moral law, based on rationality.

It is a theory of ethics proposed by a German philosopher, Immanuel Kant, in 1785, which suggests that there can be a universal moral law, or categorical imperative, that can guide the moral action of all humans. Humans are seen as being capable of rationality (on which morality should be based) and a Good Will. We therefore have the freedom and autonomy to behave rationally, and is so doing become more than subjects to moral law, but also the authors thereof. To understand this statement, consider the proposed categorical imperative: The only moral principles that we should act on, are those that we would want everyone in the world to act on, including towards us.

This requires two steps from us:

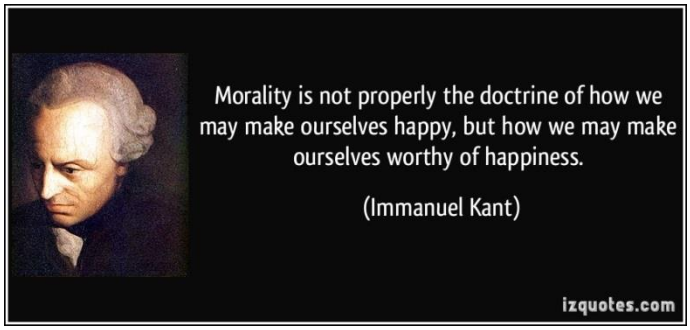
a. Ask yourself: On which principle am I basing my decision or action?
b. Ask yourself: Can I will everybody in the world to act on this same principle as a moral law?

If you answer 'yes' in step two and act accordingly, you become a creator or author of moral law. It is in this freedom that we find our human dignity.

Kant also insists that everyone has to be treated as an *end*, and not as *means* to an end.

A reworked, but easy-to-remember interpretation of Deontological Ethics is this Golden Rule: Always treat others as you would want them to treat you.

The Oxford Dictionary of Philosophy (2005) explains: "In some moral systems, notably which of Kant, real moral worth comes only with acting rightly *because* it is right. If you do what you should but from some other motive, such as fear or prudence, no moral merit accrues to you".



15. Digital divide

Digital divide refers to the gap between the information rich and the information poor.

Digital divide is defined by the OECD (2001) as "The gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities. The digital divide reflects various differences among and within countries."

Measuring Digital Divide

While the presence of communication infrastructure, computer availability and internet access are important indicators for measuring the digital divide, the implementation of such technologies will not ultimately solve the inequalities between those who have access to ICTs ("information rich") and those who do not ("information poor"). Other household factors such as income, education level, household size and type, age, gender, racial and linguistic backgrounds and location also play an important role in understanding how to bridge the digital divide (OECD, 2001).

Image: itgsopedia.wikispaces.com

16. Digital revolution

A revolution takes place when that which empowers (the means of empowerment) shifts, and the shift threatens the power strata of a society. Digital Information and Communication technologies might be causing such a shift.

Social revolutions have taken on different forms, from shifts that were mainly political, to shifts caused by technological advances during the Industrial Revolution. Revolutions have turned monarchies into democratic nation states. It has emancipated serfs and led to private land ownership, mechanised tasks that would otherwise require hard physical labour and taken people off farms and turned them into factory workers. Factory workers became machine operators. Today millions of people do not work with material objects, but with digital information. Technological and political revolutions go hand in hand in shaping society.

We cannot be sure what implications the digital revolution will have for how society is structured in the future, but it has already become clear that this revolution too has its "haves and haves not" segments of society that become respectively empowered and disempowered. There are new kinds of creators and consumers. The divide between those who have access to information as well as the skills to manipulate it and those who do not, is generally referred to as the "digital divide". The divide is not only between groups in a society, but between the 'developed and developing' nations of the world. The digital revolution will have economic, social and political implications – much of which will be guided by who takes the lead in Information and Communication Technologies.

Image: http://bsr.london.edu

17. e-Governance

It is the application of ICT by governments in order to improve service delivery (Prathab & Girish, 2006; UNESCO, 2010).

What is e-Governance?

E-Governance takes place when a government uses Information and Communication Technologies (ICTs) like the Internet, Local Area Networks and mobile devices for the exchange of information between itself and the society it serves.

What does e-Governance hope to achieve?

The idea is that e-governance methods should:

- Make government services accessible, convenient, efficient and transparent
- Be the biggest enabler of changes in process reforms with the least amount of resistance
- Increase public trust and empower the public to hold government accountable (since knowledge is power).

What is happening in Africa?

UNESCO is collaborating with the Commonwealth Network of Information Technology for Development Foundation (COMNET-IT) to promote the use of ICTs in African municipalities, through training and enablement.

How does e-Governance differ from e-Government?

An e-Government is one that actively employs e-Governance, i.e.: various ICTs for day-to-day functioning among its branches for communication and the integration of its stand-alone services.

18. e-Trust

"*In e-Trust, the thing trusted is an ICT system consisting of computers, networks and operators"* – (Nickel, 2011).

The key to understanding e-trust is that it differs from trust in a person.

A person can think and act rationally or irrationally, morally or immorally, and make decisions based on emotions and facts, and can be constantly fluctuating in their beliefs, depending on their level of integrity and moral development.

In e-trust the thing you trust is non-human. It can only act according to its hardware and software specifications. Once the ICT device becomes operational it becomes an entity incapable of acting outside of its set boundaries. Even in cases of machines programed with artificial intelligence to adapt to user preferences, it is still limited to the extent it is programed with. When we choose to trust a person we can adapt our level of trust in that person according to the feedback we receive or behaviour we observe. When we trust an ICT device or program, we can only rely on our experience with it. We are often coerced into trusting a program when we have to accept terms of use or user licences, even before we have had the opportunity to use the program.

In the electronic world we would like to trust that (a) Data will behave, (b) the personal device we use will be user-transparent, (c) intelligent software agents will behave, and (d) that intermediary identity devices will behave. In this way e-trust differs from online trust. Online trust refers to people trusting each other in an online environment.

Image: kristinnoelle.com

19. e-Waste

Electronic waste or e-waste describes discarded electrical or electronic devices.

E-waste is defined by Erasmus (2009) as "Electrical or electronic equipment which is waste, including all components, subassemblies and consumables which are part of the product at the time of discarding. It includes computers and entertainment electronics consisting of valuable as well as harmful toxic components".

Electronic information is presented on electronic equipment and devices that are discarded when they become outdated. Because of the rapid pace of the development of new ICTs, many electronic devices like mobile phones become outdated very quickly. This leads to a huge disposal problem – how do we get rid of all the devices, in other words, how can we handle e-waste? Some solutions are to recycle or reuse electronic components of hardware.

One major problem is that the so called 'developed world' has e-waste dumps in developing countries. These countries are sometimes paid for the space used for dumping e-waste, but they do not have the infrastructure to protect the environment and people in the vicinities of the dumps. In this way companies externalise the non-financial costs of their end-of-life responsibility for products.

Guiyu, in Guangdong Province of China, is said to be the largest e-waste dumpsite in the world. Nicknamed the "electronic graveyard", it is estimated that more that 80% of the waste found here is imported from overseas. Large amounts of e-waste are sent here as it is much cheaper to recycle informally in Guiyu than it is to implement formal recycling in developed countries with strict recycling guidelines. However, informal recycling techniques are extremely hazardous and health reports from Guiyu indicate that the children suffer from extremely high levels of lead and other chemical poisoning.

(Holmner, 2013; Time, 2013).

20. Electronic stewardship

It means being responsible for products throughout their lifetime, not just their usable lifetime.

Electronic Stewardship refers to the manner in which the manufacturers who make, distribute, use and dispose of electronic products, share responsibility for reducing the negative impact on the environment when such products are discarded. This can be done in two ways:

1. Extended Producer Responsibility (EPR)

The implementation of EPR policies in countries such as Norway and Switzerland shifts the responsibility of "end-of-life management" of electronic products back to the manufacturers/producers. Through these policies, manufacturers take on further responsibility to take back and dispose of products in an environmentally safe manner at the end of their lifespan. In addition, EPR policies also offer incentives to producers to take into account more environmental considerations in their product design (EPR Working Group, 2003; OECD, n.d.).

2. Advanced Recycling fee (ARF)

ARF is another manufacturer model to assist with end-of-life management. The ARF model requires that an additional fee is charged at initial purchase of product. This additional fee goes towards the cost of formal recycling of e-waste at the end of its life. In some countries, this fee can also be subsidised by government (Williams, 2010).

Exercise	
Step 1	Read this concept in conjunction with "e-Waste"
Step 2	Discuss: What does "stewardship" mean?
Step 3	Discuss: How have you disposed of your old mobile phone or computer? Was this responsible? Why or why not? Would you mind paying an extra fee for the sake of recycling of your appliance when you are not using it anymore?
Step 4	Discuss: How can you become a better steward of your electronic appliances?

21. Ethical hacking

The phrase 'ethical hacking' refers to hacking without malicious intent.

Prof MS Olivier from the Department of Computer Science at the University of Pretoria explains:

“The question whether intent is benign or malicious is not always an easy one to answer. The intent of someone who hacks into a bank's systems purely to steal money is clearly malicious. The intent of someone who hacks into his or her own system to recover data that belongs to him or her, but where the password to access the data has been forgotten is benign. However, even this latter example may move into somewhat less clear territory if the owner of the data needs to reverse-engineer parts of the system where the licencing conditions or even legislation prohibits such reverse-engineering. A more extreme example is where a hacker breaks into a corporate system and, say, defaces their website with the claim that it is in the public interest to expose those companies who do not properly secure their systems because such companies potentially put the public at risk by storing individuals' data on systems that a hacker with `real' malicious intent can compromise”.

The term “ethical hacking” can be misappropriated. To make a moral judgement on this issue not only requires more than knowledge about ethics, but also technical knowledge. This is an example of how Information Ethics (IE) poses a huge challenge to those who wish to explore it.

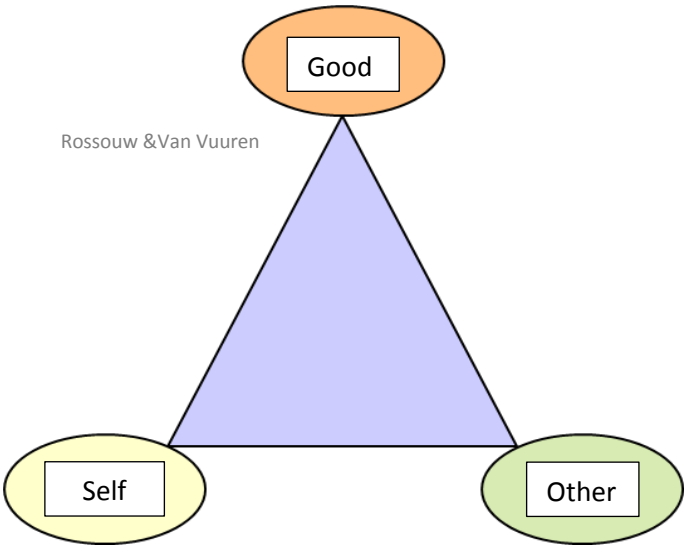
Image: office.microsoft.com

22. Ethics

Ethics is the study of morality.

Ethics is mostly studied in the fields of Philosophy and Theology and seeks to investigate how we ought to live in relation to each other in order to be happy, dignified humans.

It investigates what is good or bad (or wrong/right) about human behaviour, and more specifically why it is so. It is concerned with values and norms, and considers issues like justice, fairness and sustainability. The Oxford dictionary of Philosophy defines ethics as "the study of the concepts involved in practical reasoning: good, right, duty, obligation, virtue, freedom, rationality, choice. Also the second-order study of the objectivity, subjectivity, relativism, or scepticism that may attend claims made in these terms" (Blackburn, 2005). It is a field of study that considers and compares approaches from various theories (like Deontology, Utilitarianism and Virtue ethics), cultures and religions. In its applied form, Ethics seeks to question and understand the balance of interests between stakeholders. Rossouw and van Vuuren (2004:3) explain: "Ethics concerns itself with what is good or right in human interaction. It revolves around three central concepts: 'self', 'good', and 'other'. Ethical behaviour results when one does not merely consider what is good for oneself, but also considers what is good for others. It is important that each of these three central concepts be included in a definition of ethics". Ethics as a study of morality can be applied to various fields like information science, medical science, research practice and business practice. Information Ethics is form of applied Ethics.



23. Fraud

Intentionally deceiving someone in order to gain unfair advantage, or to cause a loss to the person you deceive.

Problems that we already face in the physical world are present in the cyber world as well. It is important to understand what fraud is, since it is a particular form of abuse of information and one form of it, namely Identity theft and fraud, has become a noteworthy problem in the Information Age.

Fraud can take place when:

- Information which should be made available is hidden
- When false information is presented

Fraud is:

- intentional
- a cause of unfair gain or loss
- dishonest
- motivated by a reward or unfair advantage for the fraudster

Fraud is bad because it:

- increases the costs of running a business, which undermines competitive business (for example: The money being spent on dealing with phishing in the banking sector)
- stimulates corruption in public and private sectors
- undermines trust in a society

Like other crimes, fraud is said to have three dimensions, namely: Motive, opportunity and rationalisation (Rossouw & van Vuuren, 2004).

Tip: Read this in conjunction with "Identity Theft and Identity Fraud"

24. Globalisation

It is the process of the increasing interconnectedness of countries around the globe.

Globalisation is driven by the increasing flow of information, goods, money and people across national borders – all of which is made possible by the development of new technologies and the freedom of mobility.

Because the world is connected, a local event can have a global impact – especially in terms of financial markets. National economies become subject to international patterns of consumption, global financial markets, multinational corporations and international trade agreements. International political bodies are also formed in the process of globalisation, like the United Nations and League of Nations.

Globalisation generates a global cultural system and a social awareness of the world as a single place, which, together with the international flow of information and goods creates the possibility for cosmopolitan lifestyles, as if found in most major cities across the globe.

25. Hacking (and related terms: Hacker, Cracker, and Penetration Testing)

Hacking is the process of obtaining access to a device or digital system using techniques or mechanisms that were not intended to provide access.

Hacking may take on different forms depending on the motivation of the hacker. The Merriam-Webster online dictionary describes a hacker as "a person who illegally gains access to and sometimes tampers with information in a computer system". Someone who commits criminal hacking is also referred to as a cracker.

Prof MS Olivier from the Department of Computer Science at the University of Pretoria explains the difference as follows:

"The hacker may attempt to gain access to (parts of) a system to which he or she has not been granted access for reasons ranging from pure curiosity about how a system works to gaining access to commit some crime. The intent and extent of a hacking attempt is seen as very important by many people who refer to themselves as hackers. Hackers who hack out of curiosity and limit their activities that are not intended to cause harm to any party prefer that the term 'hacking' should be reserved for what they do, and the term 'cracking' used for breaking into a system with malicious intent - or even hacking into a system without due care to not cause any damage. The distinction is also present in a number of phrases that distinguish between the two types: White Hat hacking, for example, refers to hacking without malicious intent, while black hat hacking refers to hacking with malicious intent".

Hacking could also be commissioned by companies for the sake of penetration testing of their digital networks. Prof MS Olivier explains: "Hacking is performed professionally by pen testers (penetration testers or, using a term that is no longer popular, tiger teams). Pen testers are employed by companies to attempt to hack into (a specific part) the company's system to test the company's system security. In order to ensure valid results, most of the staff of the company will not be aware of a pen test that is to be conducted. The nature and extent of the pen test are contractually determined prior to the initiation of the pen test".

Hacking should clearly not be used as a static term without consideration of the context in which it takes place and the motivation of the hacker.

26. Identity theft and identity fraud (refer to *fraud*)

Identity theft is when personal details of an individual are stolen and identity fraud is the use of those details to commit fraud.

In the current technological environment, one of the biggest issues of intentional falsification of information is identity theft. Identity theft occurs when someone knowingly and intentionally steals your personal information. This can be done through physical theft of wallets containing identifying documents and bank cards; "dumpster diving" to find personal information on discarded documents outside homes or businesses; digitally intercepting personal information shared online through personal communications or online business transactions; or "shoulder surfing", where an identity thief stands close enough to you during a personal transaction that they can see the personal information you are completing, for example at an ATM (Justice.gov, n.d.; SAFPS, 2008; SAPS, n.d.).

Identity fraud is when the identity thief uses the personal information stolen from you to impersonate you. This is done to conduct a wide range of crimes, from false applications for loans and credit cards to fraudulent withdrawals from bank accounts, or obtaining other goods or services which the criminal might be denied if he or she were to use his or her real name.

Identity theft is a crime. Identity theft and identity fraud can be summarised as terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain (Justice.gov, n.d.; SAFPS, 2008; SAPS, n.d.).

Clues That Someone Has Stolen Your Information
(http://www.consumer.ftc.gov/articles/0271-signs-identity-theft)

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.

27. Information

Information is organised or structured data that becomes meaningful.

Rowley and Hartley (2008) define information as "organized or structured data, which has been processed in such a way that the information now has relevance for a specific purpose or context, and is therefore meaningful, valuable, useful and relevant."

Information can be presented in verbal, written, typed, painted, sculpted, sung, gestured, animated, acted, or digital formats, among others. Some of the characteristics of information include that it is accurate and timely; specific and organised for a purpose; has context and meaning; the facts or material required to solve a problem; and can reduce uncertainty (Debons, 1988; Spiegler, 2003; Business Dictionary, 2013).

Information can be generated through research and experience; it can be shared, hidden, modified, analysed, synthesised, and manipulated. Information can become outdated. Information can be bought and sold. A piece of information is considered valueless if, after receiving it, things remain unchanged. Therefore information exists in the eye of the beholder; the same data can become nonsense to one person and gold to another (Spiegler, 2003).

Information Professional vs. Information Practitioner

The distinction between Information Professionals and Information Practitioners is still under debate. The Department of Information Science at the University of Pretoria presently distinguishes between the two as follows:

Both information professionals and practitioners are individuals who preserve, organise, and disseminate information. However, an Information professional is skilled in the organisation and retrieval of recorded knowledge, and usually has a professional qualification, for example a degree in Library and Information Sciences/ Information Studies. An information practitioner is an individual who engages in an information based profession, but does not necessarily have a formal qualification in Library and Information Sciences/ Information Studies.

28. Information Age

A new historical age that is mainly characterised by the central role of information in society.

An "Age" refers to a historical time period. For example, in the past there has been what was called the Dark Ages, the Middle Ages and the Industrial Age. Today, it is said that we have entered a new historical age, which is characterised mainly by the central idea of "Information" and how we deal with it.

The Information Age can be defined as "a period beginning in the last quarter of the 20th century when information became easily accessible through publications and through the manipulation of information by computers and computer networks" (WordNet.princeton.edu).

The Information Age is characterised by concepts that are explained elsewhere in this workbook, namely:

- A new type of economy: Refer to *Knowledge Economy*
- New structures in society: Refer to *Information and Knowledge Society*
- A new type of citizenship: Refer to *Cyber Citizen*
- A new type of warfare: Refer to *Cyber Warfare*
- A new type of poverty: Refer to *Information Poverty*

29. Information and Communication Technologies (ICTs)

ICT refers to technologies that provide access to information through telecommunications, including real-time communication options.

It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, satellite technology and other communication mediums (TechTerms, 2013).

ICT 4 D

One of the goals of ICT4D is to help reduce poverty in developing countries by researching the circumstances under which ICTs may alleviate both physical and information poverty. The Collective and Multi-disciplinary Centre for ICT for Development (ICT4D) at Royal Halloway, University of London is one of many official research centre established to research and teach appropriate and sustainable use of ICT for development. The centre was awarded UNESCO chair status in 2007, and has hosted a number of successful conferences aimed at providing a forum for researchers, practitioners and all those involved in the field of ICT development. (ICT4D, 2013; ICTD, 2010; UNITeS, 2004).

30. Information and Knowledge Society

A society where most of the workforce is engaged in the processing of information.

An information society is one in which both quality of life and economic development depend largely on the exploitation of information (Martin, 1988). In such a society, the advances in information and knowledge, including technologies associated with these advances, influence the market place, education system and work and leisure related activities. According to Martin (1988), it is a society that is reliant on information and knowledge for physical, mental and economic survival.

Over the years, a shift in emphasis was seen from simple information technologies to knowledge technologies that place more value on human capital and encourage more collaboration and interaction within the economics of information. This focus on human capital within an information society was described as the Knowledge Society (Lor & Britz, 2007). However the similarities between the information society and knowledge society showed that the two terms could not be in considered in isolation from each other. From this, the term information and knowledge society was developed to describe "A society that is reliant upon a sophisticated physical and ICT infrastructure for the improvement of everyday living and working conditions. A society that values the importance of information as a key to economic wealth and prosperity and where there is an increase in information related activities, as well as an enhancement of human intellectual capability. The information and knowledge society ensures the freedom of information through the use of information and communication technologies. In such a society, modern information and communication technologies are utilised to achieve the interaction and exchange of information between their local knowledge system (tacit knowledge and explicit knowledge) and the global knowledge system (explicit knowledge) to create usable, relevant contextualised content and knowledge. This interaction and exchange of data information and knowledge will, in turn, ensure the respect of other people's beliefs, values, norms and religions due to the increase, and availability, of information regarding these aspects" (Holmner, 2008).

31. Information anxiety

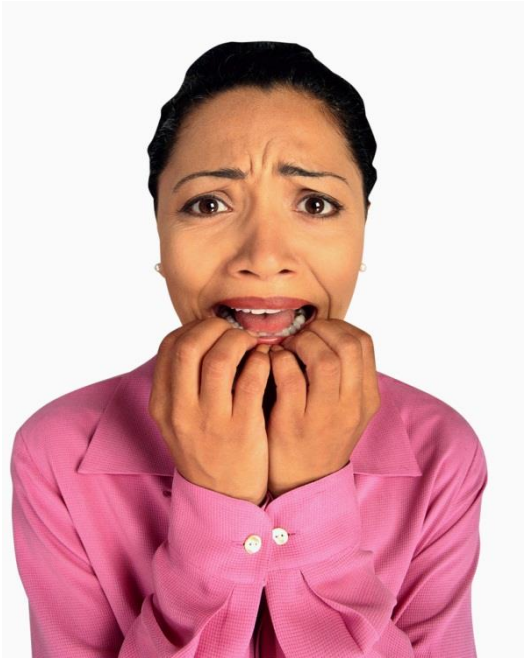
Anxiety caused by our emotional relationship with information.

“Information Anxiety is produced by the ever-widening gap between what we understand and what we think we should understand. It is the black hole between data and knowledge, and it happens when information doesn't tell us what we want or need to know” (Wurman, 1989).

Wurman (1989) further points out five subcomponents of information anxiety:

1. Not understanding information;
2. Feeling overwhelmed by the amount of information to be understood;
3. Not knowing if certain information exists;
4. Not knowing where to find information;
5. Knowing exactly where to find the information, but not having the key to access it.

Where the above five subcomponents are present most of the time, it is likely to be the scene of either information overload or the result of *information poverty*.



32. Information appliances

They are the electronic devices we use to manipulate (create, find and share) information.

Wisegeek.com (2003) offers this definition: An information appliance can be any portable computing device capable of transferring data to or from another device. It usually performs multiple specialised tasks, such as the calendar, notepad and phone book functions of a Personal Digital Assistant (PDA). The core of an information device is usually an embedded system rather than a complete laptop or desktop motherboard. Information appliances include telephones, notepads and mobile web browsers.

Internet access is not required for a device to be considered an information appliance, but it is frequently a feature. More important is the ability to transfer data to and from the appliance over some sort of connection. It can utilise a wired Ethernet port or Universal Serial Bus (USB) link for this. It may also include wireless network capability, either directly to the Internet or to a local area network (LAN).

The main function of an information appliance is usually to retrieve and manipulate data, for either business or consumer purposes. To do this, it must include some means of input and display for its user, usually more limited than that of a laptop computer. Depending on the intended use of the device, it may have a specialised keyboard and display. Some units include a touch screen and stylus for data entry. Once the components are disposed of, they become e-waste.

Image: extremetech.com

33. Information Ethics (Read in conjunction with *Ethics*)

A branch of applied ethics that studies what is morally good or bad, specifically in the context of the handling of Information, and the Information Age.

Information Ethics is a branch of applied ethics (refer to *Ethics*). IE deals with issues like justice, fairness, freedom and human dignity and what is morally right or wrong on three levels:

(1) Macro level: The broad social and environmental issues attributed to the features of the Information Age (like the Digital Divide and e-Waste),
(2) Meso level: Questions arising in the sphere of public policy, discourse and regulation of information (like Censorship), and
(3) Micro level: The day-to-day handling of information throughout the Information life-cycle (like Plagiarism).

IE topics include *Information and ICT based*:

- *conditions* (information- poverty, literacy, access)
- *crimes* (cracking, identity theft/fraud)
- *experiences* (information- overload and anxiety, cyberbullying)
- *rights and responsibilities* (information privacy, cyber-citizenship, social responsibility, accountability etc.)

According to the African Network for Information Ethics, "Information Ethics is a relatively new concept that developed as part of the growing availability and use of ICTs [and studies] the changes in the relationship between people and the world due to information and communication technologies". Essentially, ancient, modern and contemporary approaches to ethics are employed to address current, developing and foreseeable ethical issues that arise with the increasing prominence of the role of information and ICTs.

34. Information Integrity

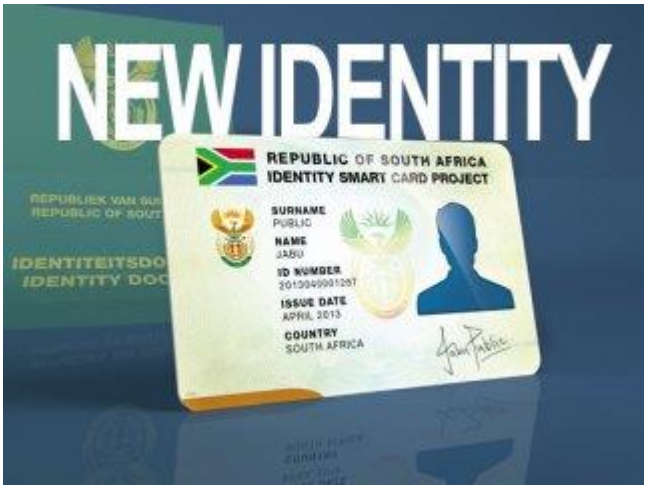
Information integrity refers to the assurance that information has not been modified from its original source.

According to Trites (2011), "Information integrity includes the accuracy, relevance, precision, timeliness and completeness of the information and its meta-information. Information that is accurate, relevant, precise, timely and complete for a particular purpose can be termed to be "fit for purpose".

Information (or data) integrity refers to the validity and reliability of information. It ensures that data remains consistent and accurate, and that it has not been changed accidentally or intentionally from the source. It may also refer to the protection of information from unauthorised access and alteration, through the use of policies or physical technologies.

South Africa – Smart Identity Document Roll Out

"The ID smart card is a way of affirming citizenship and using digital technology to protect the integrity of our identity as South Africans." – Naledi Pandor, 2013



35. Information life cycle

Information is dynamic and has a lifecycle.

According to McGilvray (2008) the information life cycle consists of six phases, namely: Plan, Obtain, Store and share, Maintain, Apply, and Dispose. The acronym POSMAD can be used to remember the steps of this non-linear lifecycle.

The following table, taken from McGilvrey (2008), illustrates the phases of the information life cycle, with examples:

Information Life Cycle Phase (POSMAD)	Definition	Example Activities for Information
Plan	Prepare for the resource	Identify objectives, plan information architecture, develop standards and definitions. When modeling, designing, and developing applications, databases, processes, organizations, etc., many activities could be considered part of the Plan phase for information.
Obtain	Acquire the resource	Create records, purchase data, load external files, etc.
Store and Share	Hold information about the resource electronically or in hardcopy, and make it available for use through a distribution method	Store data electronically in databases or some type of file, or store as hardcopy such as a paper application form. Share information about the resource through networks, an enterprise service bus, or e-mail.
Maintain	Ensure that the resource continues to work properly	Update, change, manipulate, parse, standardise, validate, or verify data; enhance or augment data; cleanse, scrub, or transform data; de-duplicate, link, or match records; merge or consolidate records, etc.
Apply	Use the resource to accomplish your goals	Retrieve data; use information. This includes all information usage: completing a transaction, writing a report, making a management decision from information in those reports, running automated processes, etc.
Dispose	Discard the resource when it is no longer of use	Archive information; delete data or records.

36. Information literacy

Information literacy means that you can identify, evaluate and use information effectively.

Information literacy should not be confused with computer literacy.

To operate effectively in an Information and Knowledge Society, you need to be information literate. The following specific skills or abilities are essential to be considered information literate (Auckland, 2002; Bothma et. al ,2009; Bruce, 1999; Mason, 1986; SKIL, 2013):

- Knowing where to find relevant information and having access to it;
- Knowing how to critically evaluate and sift through available information;
- An awareness of your personal and professional ethics;
- The ability to evaluate and organise information (reliable vs. unreliable);
- An understanding of information needs;
- The ability to interact with information professionals;
- The ability to use information for decision making, task completion and problem solving;
- The ability to use information effectively in research;
- An awareness of legal issues surrounding the use of information;
- The ability to access the information technologies which store, convey and process information;
- Synthesise and build on existing information.

Information literacy also includes the ability to build up a personal knowledge base and gain new insights, as well as using information wisely to the benefit of others (Bruce, 1999).

Tip: Discuss in conjunction with “Digital Divide”

37. Information overload

Being confronted with so much information, relative to the amount of time it is presented in, that you cannot think clearly.

You will experience an information overload when:

- You receive such a *large quantity* of information that you cannot sift through it efficiently, memorise it, or make sense of it.
- You receive information at such a *quick pace* or in such a short span of time that you do not have enough time to categorise the information as you receive it, for instance, establishing whether it is relevant or irrelevant information.
- You receive information, regardless of quantity or pace, without having the necessary *ability* to cope with information as you receive it. In other words, you do not have the necessary skills to categorise, analyse and synthesise information.

Consequences of information overload:

- It can make it very difficult to make an informed decision.
- It can undermine the principle of informed consent.
- It can make it extremely difficult to make an ethically sound decision in morally complex situations like moral dilemmas.
- It can make it difficult to make swift decisions, even in relatively uncomplicated ethical matters.

Coping with information overload requires you to build the necessary cognitive and practical skills for information processing (Cambridge Dictionary, 2013).

38. Information poverty

It is a state where people suffer from a lack of information, as one would suffer from a lack of money or resources.

'Poverty' is relative to 'wealth', and as with money, information poverty leaves you in a disadvantaged position is society (Murdock and Golding, 1989).

Johannes Britz (2004) defines information poverty as "that situation in which individuals and communities, within a given context, do not have the requisite skills, abilities, or material means to obtain efficient access to information, interpret it and apply it appropriately. It is further characterised by a lack of essential information and poorly developed information infrastructure".

Information poverty occurs when a person's ability to access and benefit from information is hampered by factors like:

- Level of education, especially the skills needed to use ICT, and fluency in English – since this is the dominant language of ICT programing.
- Governmental policies, cultural and religious beliefs which discourage access to information by, for instance severely censoring the internet, or only providing education to men and not to women.

To avoid information poverty, people need to be equipped with knowledge about knowledge, like how to find, use and determine the validity of available information.

Tip: Discuss in conjunction with "Digital Divide"

39. Information Privacy

Information privacy is the protection of personal information from publicity.

Information Privacy refers to the link between collection and dissemination of personal data; the use of technology in the collection and management of information; individual expectations of privacy in society, and the political and legislative issues surrounding these issues (OECD, 2013).

In order to fully understand what information privacy is meant to protect, you must first familiarise yourself with what is considered as personal data/information. This includes:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history or the person;
- any identifying number, symbol, email address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person.

Thus, information privacy refers to the protection of personally identifying information and the ability of an individual to control the release of such information in the public domain.

Refer to: The Protection of Personal Information Bill No 9 of 2009

In South Africa, the Protection of Personal Information Bill (No 9 of 2009) is a piece of legislation that is designed to protect citizen's constitutional right to privacy, through safeguarding personal information by setting safe conditions for how information may be processed. It aims to balance the right to privacy with other rights such as access to information. The aim of the legislation is to monitor the way in which personal information is collected and processed, and enforcing harsh penalties for those who do not comply.

40. Information System

A broad term referring to a computerised or manual system dealing with data and information.

Information systems are defined in different way depending on the discipline and purpose for use. Regardless of the definition however, information systems mainly focus on four components, namely people, strategy and organisation, business processes, and information and communication technologies. These components all need to be considered when selecting or developing an information system in order to meet the information needs of an organisation and its people (employees, clients, customers etc.) (Chaffey & White, 2012; UCT, 2013).

The following definition is a combined definition for information systems:

An information system is a manual or information technology based system, used by organisations and people to capture, process, store, use and disseminate data and information, in order to address the needs of an organisation (Chaffey & White, 2012; UCT, 2013).

More definitions

- Wordnet: A "system consisting of the network of all communication channels used within an organisation".
- Business Dictionary.com: "A combination of hardware, software, infrastructure and trained personnel organised to facilitate planning, control, coordination, and decision making in an organisation".
- University of Cape Town: "Information Systems are a means by which organisations and people use computers to collect, process, store, use (analyse) and distribute information".
- Britannica Online Encyclopaedia: An "integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products. Business firms and other organisations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. For instance, corporations use information systems to reach their potential customers with targeted messages over the Web, to process financial accounts, and to manage their human resources. Governments deploy information systems to provide services cost-effectively to citizens"

41. Informational Self-Determination

Having control over the information about ourselves that is distributed, and also how and where to it is distributed.

Ann Cavoukian (2008:89-90) describes it as "the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal information" and that this "forms the basis of modern privacy laws and practices around the world".

Discussion Exercise

1. How important is "Informational Self-Determination"?

2. Why is it important/unimportant?

3. How do you feel when it is undermined? (For example when you get promotional phone calls from companies that you did not give your name and number to).

4. Do you think Informational Self-Determination should be a human right, or would that be taking it too far?

5. What steps can you take to protect or enhance your Informational Self-Determination?

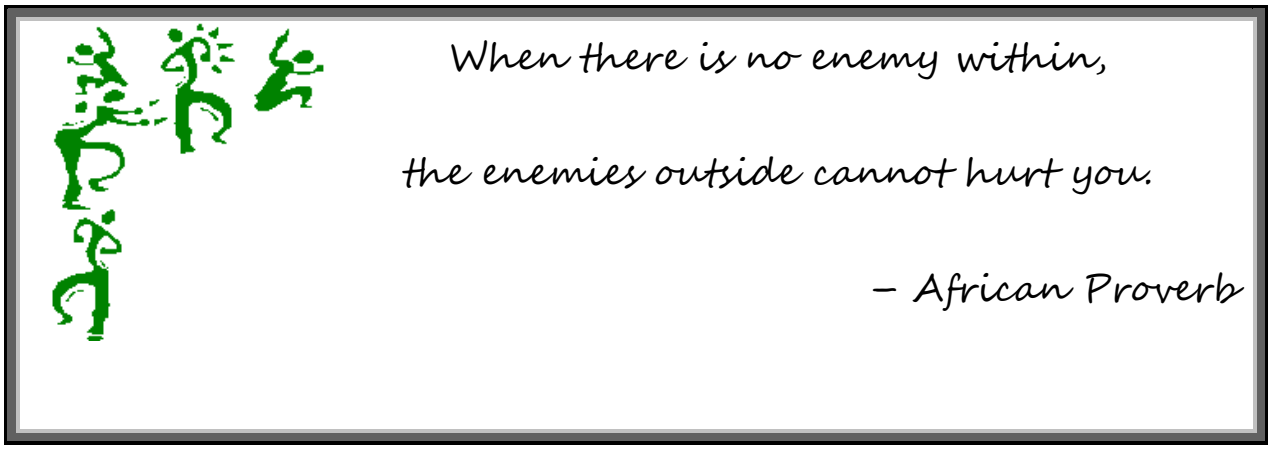
6. What steps can you take to protect or enhance the Informational Self-Determination of others?

7. Do we have a moral duty to protect or advance Informational Self-Determination? Why or why not?

42. Integrity (as *personal* integrity)

Integrity is about keeping your behaviour in line with your moral values.

A person with integrity acts consistently according to his or her strongly held moral convictions or values. The result is that one can more or less reliably predict the types of choices a person will make, given that you are aware of their value-set. Persons with perceived integrity are likely to be seen as reliable and trustworthy. There is a sense of wholeness about them because their beliefs and actions are in line with one another.



43. Intellectual Property

"Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce" (WIPO, 2012).

"Intellectual property" consists broadly of two main branches (WIPO, 2012):

- industrial property, which mainly vests in inventions, patents, innovations, trademarks, industrial designs and models, trade secrets and expertise; and
- copyright, which mainly subsists in written, electronic and other forms of information, musical compositions, computer programs (software), and artistic, photographic and audio-visual creations.

Protection of Intellectual Property Rights: Piracy

Intellectual property rights (IPR) are intangible (immaterial) property rights which are the results of creative works intellectual effort. They are primarily derived from legislation that protects the ownership and distribution rights around patents, designs, copyrights and trademarks (WIPO, 2012):

One example of an infringement of IPR is piracy. Piracy refers to the act of unauthorised duplication and distribution of materials protected by IPR. With the rise of digital technologies and internet sharing sites, piracy is becoming an increasing problem. The enforcement of laws against infringements such as Piracy is becoming more difficult, as technologies create methods for easy reproduction and policy makers are struggling to deal with the mind-set of the cyberspace community, who follow a more altruistic attitude of sharing information and ideas freely over networks.

44. Intellectual Property Topics of Interest

a. Open Access Initiative

The Budapest Open Access Initiative is a framework of acceptable principles for open access.

As more people gain access to computers and internet connection, there is a growing demand to provide the public with free, unrestricted access to academic research through the open access movement. In order to achieve this, the Budapest Open Access Initiative encourages the development of open access policies in higher education institutions and funding agencies, the open licensing of academic works, the development of open access repositories, and standards for open access publishing (Budapest Open Access Initiative, 2013).

b. Creative Commons

Creative Commons supplements copyright by enabling an organisation or individual authors to modify copyright terms to suit their needs.

Creative Commons is a non-profit organisation that was established in 2001 with the aim of providing the means for the public to share, build on and use creative works, without the traditional copyright restrictions. It does this by offering six types of licenses for authors to share copyrighted work on their own conditions, changing copyright from "all rights reserved" to "some rights reserved" (Creative Commons, 2013).

45. Knowledge Economy

An economy focused on the generation, sharing and use of knowledge, rather than the processing of raw materials.

<u>In a Knowledge Economy:</u>

- According to (OCDE, 1996)
    - The economy is increasingly based on the production, distribution and use of knowledge and information
    - The economy grows in terms of high-technology industries
    - It is increasingly focused on highly skilled labour

- According to (WorldBankGroup, 2003)
    - The generation of ideas become more important than physical abilities
    - The development of new technologies become more important than the processing raw materials
    - It is characterised by the effective creation, finding and sharing of knowledge

- According to (Roberts, 2009)
    - There is an increase in technological and scientific advances
    - The aim is to gain knowledge that can lead to the improvement of all stages of production processes

46. Marginalisation

Being pushed out of the mainstream and into the periphery of society and losing the associated benefits of mainstream citizenship; being left behind because of policies or processes that are not inclusive.

People are marginalised when they are cast into the periphery of society through policies and practices that directly or indirectly disempower them. Marginalised people are often women, children, the elderly, the disabled, ethnic minorities, or today, it could be argued, those without sufficient access to information. By extension, the illiterate are likely to become marginalised. Sometimes the marginalised people of a society constitute a numerical majority – as was the case in Apartheid South Africa.

Marginalised people cannot fully or effectively participate as citizens. As groups they are left voiceless and are unrepresented or underrepresented where social policy decisions are made.

If access to information becomes necessary for active citizenship, then those without access to information are likely to become marginalised in society.

47. Moral development

The formation and maturation of a sense of right and wrong.

The moral development of an individual follows much the same route as her physical, emotional and cognitive development does – it matures.

We are socialised into certain moral frameworks from a very young age, but how we relate to these frameworks changes as we grow, either in age or in experience.

Velasquez (1998) points to three general stages of moral development:

1. In the first stage, as a child, we are told what is right and what is wrong, and we try to do what is right in order to avoid punishment.
2. In the second stage, we begin to internalise moral standards, which means that it becomes our own, to the point where it becomes part of our personal identity. In this stage, we try to do what is morally right in order to live up to the expectations of those around us.
3. In the third stage, we begin to critically reflect on moral standards. We begin to rationally consider their consequences, and to revise them accordingly. At this stage, we begin to 'do ethics'.

According to this approach, our moral development can be measured against our ability to balance taking care of ourselves with taking care of others as a way of life.

Discuss: This approach is based on Western Philosophy and Developmental Psychology. How would this fit in with an African concept like Ubuntu?

48. Moral dilemma (or ethical dilemma)

A moral dilemma occurs when you have to make an ethical decision where whichever choice you make will cause you to do something morally wrong (McConnell, 2010).

Moral or ethical dilemmas occur because of different values that do not allow you to honour the one without dishonouring the other. If an overriding value or principle were present, there would be no moral dilemma. In a moral dilemma the contesting principles or values are equally important. Conflicts of values occur between moral reasons and reasons of law, religion and self-interest. In a moral dilemma you have a moral obligation to do two or more things, and you can do each on its own, but it is impossible to do both. No matter what you do in this situation, you are doomed to moral failure. Ignoring one is unethical in one way, ignoring the other unethical in another. In this way your only options could both be unethical in some way (Hughes, 2012).

A tell-tale sign of being caught in a moral dilemma is feeling some guilt or remorse about the decision you made, even if these feelings can be rationally questioned and challenged.

Sometimes you might hear people say 'you can't make an omelette without breaking eggs'. It means that in order to achieve some result, sacrifices have to be made. When you are in a moral dilemma situation, you might end up feeling this way, or using a similar pattern of thought to justify your behaviour.

49. Moral enterprise/moral entrepreneur

Moral entrepreneurs undertake a moral enterprise by taking interest in how rules are produced and enforced and by promoting morality.

The Oxford dictionary of Sociology explains that moral enterprise "refers to the process involved in creating an awareness of issues and following them through into the statute-book".

Moral entrepreneurs actively promote morality. They are the rule-makers, campaigners and enforcers of ethics. They work to create a moral awareness, and can cause moral panic when they, together with mass media, arouse concern over a social issue.

50. Moral imagination

An ability to imagine how things could be better than they are (more ethical), that enables us to change our behaviour.

Some people feel stuck in situations where they have to take part in unfair, unethical or immoral practices, but continue to do so since they see no alternative. If they are able to imagine how things could be different and better, they can act on it to effect change. It is the ability to imagine the different outcomes of different choices, in order to make the best one. As we mature in our *moral development* our moral imagination may become more vivid.

51. Moral philosophy (as an introduction to Ethics)

It is the branch of philosophy that deals with how we decide what is right or wrong about human behaviour. It is often used interchangeably with "Ethics".

We all have some socialised, internalised sense of wrong or right that we often have a hard time putting into words – we just *know*. Moral philosophy is when philosophers start examining, talking and writing about what is wrong or right and why.

Moral philosophers question and seek to provide answers about what is 'good', and what we 'ought' to do or how to live a 'good life'. They usually begin by examining the nature of human beings – are we rational or irrational? Are we free to make our own decisions? What do we need to do in order to live with dignity? What is the purpose of human life? Is it to find profound happiness or seek simple pleasure?

They then proceed to offer theories, in the form of Ethics, based on the answers of the above questions. Some theories claim to be descriptive, in that they describe human morality. Others are prescriptive and provide guidelines for how to live a moral or good live. Moral philosophy takes into account values, norms and concepts like freedom, justice and equality. It is important to take note that "moral philosophy" is not philosophy that is 'moral' as opposed to 'immoral', but is instead the philosophy of morality. The term is often used interchangeably with "Ethics".

The diversity of theories of morality or ethics can lead to multiple answers to a single moral question, but even so, they equip us with vocabulary, perspective and insight to make our own, considered, decisions.

Tip: Read this concept together with "Ethics"

52. Moral relativism (or ethical relativism)

A view that what is right or wrong is completely subjective and that all different views are equally valid, whether they make sense or not.

Moral relativism is sometimes resorted to when there is moral dissensus and a principle cannot be universally applied and the view is taken that different things are believed to be right or wrong for different people and that everyone's differing view is valid, even though it lacks consensus.

Velasquez (1998:22) offers a useful description: "Ethical relativism is the theory that, because different societies have different ethical beliefs, there is no rational way of determining whether an action is morally right or wrong other than by asking whether the people of this or that society believe it is morally right or wrong. Or, to put it another way: Ethical relativism is the view that there are no ethical standards that are absolutely true and that apply or should be applied to the companies and people of all societies. Instead, relativism holds, something is right for the people or companies in one particular society if it accords with their moral standards and wrong for them if it violates their moral standards".

Moral relativism can easily lead to an "anything goes" approach, which is not helpful at all. Instead of reverting to moral relativism, we can rather seek to be sensitive to situated values – acknowledging that values can have different meanings or practical implications in different situations or cultures, while keeping in mind that values still belong to a larger world view of what is right and wrong, which is likely to have things in common with other world views.

53. Norms

Norms are socially acceptable standards of behaviour.

Like rules or laws, norms are prescriptive (they tell us how to behave). They may differ between various communities. Norms are standards of culturally accepted behaviour. Adherence to norms contributes to social order by creating a shared expectation of behaviour that is in line with what is culturally desirable and appropriate. A person who does not behave according to their society's norms may be seen as deviant, and their behaviour will be met with disapproval.

> *"Norms define appropriate and acceptable behaviour in specific situations. They are enforced by positive and negative sanctions which may be formal or informal. The sanctions that enforce norms are a major part of the mechanisms of social control which are concerned with maintaining order in society"*
>
> *(Haralambos & Holborn, 2000:5)*

54. Plagiarism

The practice of an individual stealing and using another author's work as his/her own.

Plagiarism refers to the illegal and unethical practice of presenting someone else's ideas or creative works as your own. It is considered intellectual theft, and in an academic context, may result in serious penalties.

Plagiarism can take a number of forms, including (UTS, 2010; UP, 2013):

- Copying significant portions of the text straight from a single source.
- Copying sentences from several different sources, and then putting those sentences together to make it look like original work.
- Changing key words or phrases to change the appearance while still retaining the source content.
- Writing an entire paper with paraphrased or directly quoted sections, with no original work.
- Copying your own work from a previous publication and resubmitting it.
- Citing the incorrect author.
- Incorrect citation of sources making it impossible to find.

According to UTS (2010), the following practices have been shown to reduce the chances of accidentally plagiarising:

- Keep a detailed list of your sources throughout the course of your research.
- Sources from which you have extracted or developed your ideas, even if you put those ideas into your own words, must always be acknowledged.
- Always use quotation marks or some other acceptable form of acknowledgement when quoting directly from a work.
- Avoid excessive paraphrasing, even where you acknowledge the source.
- Show that you have thought about the material and understood it.

55. Privacy

The right to keep your information and deeds to yourself, without being subject to surveillance.

There are four main types of privacy. These types of privacy cannot adequately describe privacy if they stand alone.

1. Physical/accessibility privacy - This refers to privacy as non-intrusion involving one's physical space.
2. Decisional privacy – refers to privacy as non-interference involving one's choices. This is freedom from interference affecting choices/decisions concerning health care, education, work, marriage etc.
3. Psychological/Mental privacy - privacy as non-intrusion/non-interference involving one's thoughts and one's personal identity.
4. Informational privacy - This kind of privacy refers to having control over/limiting access to one's personal information. Restriction on "facts" about someone that is "unknown". This can include data about one's daily activities, personal lifestyle, finances, medical history, and academic achievement.

Article 12 of the Universal Declaration of Human Rights

This declaration states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

The right to privacy is thus a universal human right that is protected by both our Constitution and the Universal Declaration of Human Rights.

56. Social engineering (in ICT environment)

The process of deceiving users so that they provide access details is known as social engineering.

Prof MS Olivier from the Department of Computer Science at the University of Pretoria explains:

Most examples of social engineering are malicious in nature and should rather be described as cracking. A pen tester who uses social engineering may be an example of social engineering being used with benign intent.

Hacking typically occurs by exploiting a vulnerability (or weakness) in a system. In many systems the human is still the weakest link and the hacking attempt proceeds by convincing a user who has access to a system to provide the hacker with suitable access details. Examples of hackers pretending to be IT service staff and claiming that they need a user's access details to repair some problem are well known, but the method still works often enough. Variations on this theme (that may be somewhat more elaborate to be more convincing) still account for a very large proportion of successful hacking attempts.

57. Social media

Digital platforms for social exchange that are characterised by User Generated Content. It is the defining feature of Web 2.0.

Media refers to instruments of communication and interaction. In this case it refers to online instruments with decidedly social applications.

Features of Social Media:

The media:

- Uses Internet or Web based applications
- Uses mobile technologies
- Uses virtual communities and networks

The social element:

- Used for the exchange of information and ideas
- It allows User-generated Content (UGC)
- It consists of highly interactive platforms
- It allows people to build relationships and have discussions in real time

Examples of Social Media Sites

- Facebook www.facebook.com
- YouTube www.youtube.com
- Flickr www.flickr.com
- Google+ https://plus.google.com/
- LinkedIn www.linkedin.com
- MySpace www.myspace.com
- Twitter www.twitter.com

58. Social responsibility (as an introduction to *CSR*)

The responsibility that an organisation has towards the society in which it operates.

The more power or influence the organisation has the more responsibility it has. The more rights the organisation has, the more responsibility it has to the society that has given the organisation its rights. The more society trusts the organisation the more responsibility the organisation has.

Example 1: Society gives the right to a democratic government to rule. Therefore government has the responsibility towards society to govern well. Social order depends on it.

Example 2: Society trusts schools and universities to provide a good education to citizens. Places of education therefore have a responsibility to provide good education. Societal development depends on it.

Since corporations (like Microsoft and Apple) are large, power wielding and influential in society, they have responsibilities towards society, referred to as "Corporate Social Responsibility" (CSR). Some people feel corporations take a lot from society and should therefore put back into society. This is not, however the main purpose of corporations which are profit driven and the pillars of the economy. Perhaps a more sensible way to look at it is for corporations to take responsibility for the damages that they do to society. For example, a mine that pollutes the water that the community uses should take responsibility for taking fresh water away from the community by giving them fresh water again – either by managing their polluting processes better, or by providing clean water in other ways.

Tip: Read this together with "e-Waste" and "Electronic Stewardship".

59. Stakeholders

All those parties (persons, organisations) that influence or are influenced by a decision.

Stakeholders can be broken down into categories, as follows:

- Internal stakeholders: Those stakeholders that are internal to the organisation. Example: When a university makes an employment policy decision, everyone who is employed by the university is considered as internal stakeholders.
- External stakeholders: Those stakeholders (persons or organisations) that are outside of the university employment circle, but are influenced by the employment policy. Example: Students who are influenced by the repercussions of the decision. They would be affected if there are less/more teaching personnel, or less/more admin personnel.

Stakeholders can include shareholders, employees, suppliers, clients, end-users, competitors, government, and the people living in the vicinity of where the natural environment is affected.

60. Sustainable development

The ability of a process to sustain itself.

According to the Brundtland report of 1987, "sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs". In order to do this, the process cannot deplete the resources it requires to function. Therefore, a sustainable practice is one using sustainable sources. Sustainable Development is seen as the basis of Corporate Social Responsibility.

Tip: Read and discuss together with "e-Waste" and "Electronic Stewardship"

61. Trust

It is an attitude where you are willing to rely on someone else to act in your best interest.

When you trust someone you also expect them to act in a way that confirms that you can continue to trust them (Nickel, 2011, p. 355).

Some authors argue that you will only trust someone if you are sure of their identity and share a common background (Turilli, Vaccaro, & Taddeo, 2012, p. 334).

Others, like Nissenbaum (Turilli, Vaccaro, & Taddeo, 2012, p. 334) argue that you are likely to trust someone in an environment where moral and cultural norms are advocated, and the betrayal of trust is dealt with by (1) making it public, (2) punishing the one who betrays, and (3) public policy that protects trust.

However, a lot of people seem to trust others in online environments where you cannot be sure of the other person's identity and there are no real measures in place to deal with the betrayal of trust. Online trust, therefore, seems to be quite different from traditional ideas of trust.

Image from www.idioplatform.com

62. Utilitarian Ethics / Utilitarianism

A moral theory that proposes that action should be so directed as to achieve maximum utility and pleasure, and to minimise pain.

Utilitarian ethics does not allow seemingly arbitrary attitudes to influence moral judgement, and does not forbid any action in particular. In classical utilitarianism 'pleasure' is good in itself, which has resulted in the theory to be labelled as hedonistic. However, it is not just the immediate effects of pain or pleasure that should be considered when making moral judgements, principles like justice are also important for long term societal happiness.

Utilitarianism requires a cost/benefit analysis or calculation to determine the right course of action. Immediate, foreseeable and indirect effects should be included so as to maximise utility or pleasure for the most number of people.

The utilitarian principle proposes that the course of action which is morally correct is the one that produces the most happiness in comparison to every other available option in that situation.

A major problem with Utilitarianism is that it leaves loopholes for inhumane actions in the name of the greater good/happiness. It is a moral theory that is perhaps better suited for use in policy making, rather than individual moral guidance.

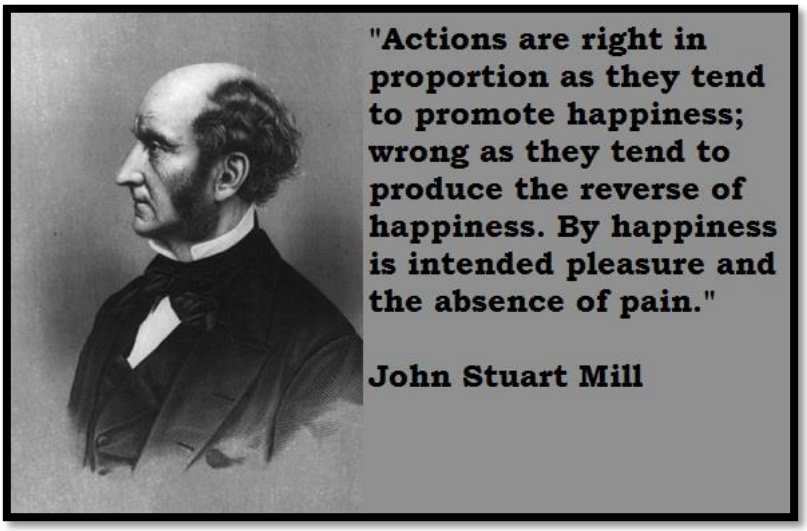


Image: rugusavay.com

63. Values (as *moral* values)

Moral values are culturally embedded informal guidelines for behaviour.

These are relatively stable convictions or beliefs about what is "important, worthwhile and worth striving for" (Haralambos & Holborn, 2000:5) that provide us with general guidelines for behaviour. Our values come from our religion, education, ideological ideas and home environment. One can have values that are not ethical. Moral values are diverse and more flexible than norms. Shared values can crystallise into norms over time.

Our values are often hard to put into words. Try to write down your own – you might find this to be a bit of a challenge at first!

64. Value Sensitive Design (VSD)

It is a framework or method for designers and developers of new technologies whereby they are urged to take moral values into consideration.

Value Sensitive Design is a framework that provides practical guidelines to the designers and developers of new technologies, to enable them to take human ethical values into account (Pommeranz, Detweiler, Wigger, & Jonker, 2012).

According to (Friedman, Kahn, & Borning, Forthcoming, pp. 12-13) VSD has four main components:

1. It aims to be proactive. It focuses on human values from the beginning to the end of the design process.
2. Values from different areas of people's lives are taken into consideration, for instance values from work, school, home, online communities etc.
3. It aims to provide a structured, theoretically sound method for designers and developers.
4. It looks beyond participation and democracy to include other moral values like fairness, justice, human welfare, virtue, etc.

VSD requires designers and developers to look beyond the 'specs' of the piece of technology or social platform they create, and to consider whether it, and its possible uses, will be respectful of human moral values. In order to use this method, designers and developers need to engage different stakeholders from the very beginning of the design process.

65. Virtue Ethics

Aristotle, a 4th century BC philosopher brought us the moral theory we know up to today as Virtue Ethics. It is a very broad philosophy that goes far beyond the meaning of 'good' or what we 'ought' to do.

According to Aristotle everything in life has a purpose. The purpose of a human being is to function in society and achieve happiness in the fullest sense of the word. In order to achieve this we need a just society, material means, good friends, and most importantly, must cultivate virtue and a moral character.

We cultivate a moral character by living according to a moral theory of moderation, since virtue is the midway between two extremes that are both vices. For instance, courage is a virtue, and it is the midway point between the two vices of foolhardiness and cowardice. In this view, natural (irrational) pleasures will not cause true happiness, because we tend to indulge in pleasures, which lead towards excess, and away from the golden mean where virtue is found and practiced.

What does the virtuous man look like according to Aristotle? Rossouw and van Vuuren (2004) summarise it as follows: It is "the man who has taken rational control of his life, has cultivated his natural dispositions into moral virtues, and has always throughout his lifetime found pleasure in acting in accordance with these virtues".

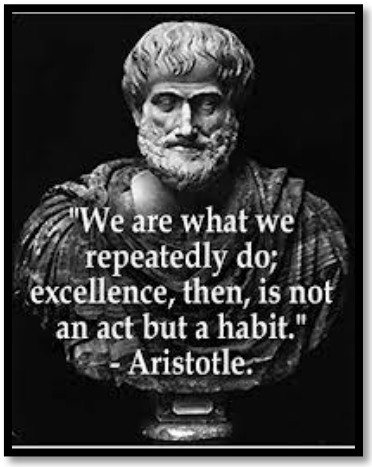


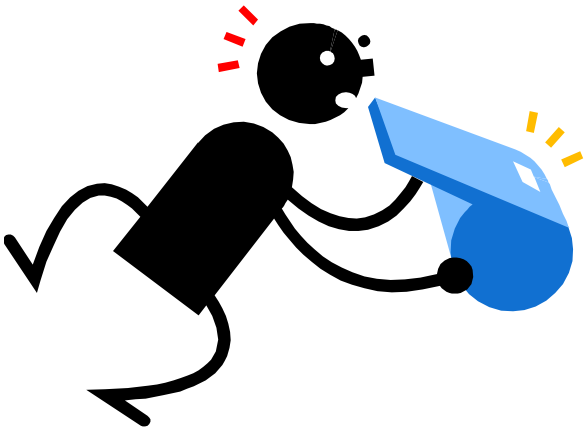
Image: http://letswatchtech.blogspot.com

66. Whistle blowing

It is a term used for what is legally known as Public Interest Disclosure.

It describes the disclosure by an employee/person (current or former) in a governmental agency or private organisation, to the public or those in authority, about malpractice, corruption, immoral acts or some wrong doing they discover that may be able to effect action (Investopedia, 2013; lse, 2012; Miceli & Near, 1984; Tavakoli et al., 2003).

- It is generally the final step when internal reporting according to normal channels fails.
- Ethics hotline: Often used for whistle-blowing. A dedicated line to report violations. Issues raised here are handled by an ethics officer.



Bibliography

- Auckland, M. 2002. Information skills in the twenty first century. *Paper presented at the First Annual Conference of the Chartered Institute of Library and Information Professionals in Scotland,* Peebles Hotel Hydro, 20 - 23 May 2002.
- *Access to information.* [Online]. Available at: http://www.education.com/definition/access-to-information. Accessed on 6 July 2013
- Blackburn, S. 2005. *Oxford Dictionary of Philosophy*. 2nd ed. Oxford University Press: Oxford.
- Bothma, T. *et al*. 2009. *Navigating information literacy.* Cape Town: Pearson Education.
- Bram, L. & Dickey, N. (Eds.) 1993. Censorship. In: *Funk and Wagnalls new encyclopaedia*. Oxford University Press: USA.
- Britz, J.J. 2004. To know or not to know: A moral reflection on information poverty. *Journal of Information Science,* 30(3): 192-204.
- Broucek, V. & Turner, P. 2013. Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud' - a forensic computing perspective. *Journal of Computer Virology and Hacking Techniques,* 2013(9): 27-33.
- Bruce, C. 1999. Workplace experiences of information literacy. *International Journal of Information Management,* 19: 33-47.
- Budapest Open Access Iniative. 2002. Read the Budapest open access initiative. [Online]. Available: <http://www.budapestopenaccessinitiative.org/read> [Accessed 6 September 2013].
- Burnett, S. & Feamster, N. 2013. Making sense of internet censorship: a new frontier for internet measurement. *ACM SIGCOMM Computer Communication Review,* 43(3): 84-89.
- *Business Dictionary*. 2013. *Definition of accountability*. [Online]. Available: <http://www.businessdictionary.com/definition/accountability.html> [Accessed 20 August 2013].
- *Business Dictionary*. 2013. *Definition of information*. [Online]. Available: <http://www.businessdictionary.com/definition/information.html> [Accessed 20 August 2013].
- *Cambridge Dictionary Online*. 2013. *Definition information overload*. [Online]. Available: <http://dictionary.cambridge.org/dictionary/british/information-overload?q=information+overload> [Accessed 29 July 2013].
- Carroll, A.B. 1999. Corporate social responsibility: evolution of a definitional construct. *Business and Society*, 30(3): 268-295.
- Cavoukian, A. 2008. Privacy in the clouds. *IDIS*, 1:89-108.
- Chaffey, D. & White, G. 2011. *Business information management.* Prentice Hall: England.
- Coetzer, P. 2013. *Cyber crime escalates in South Africa*. [Online]. Available: <http://www.leadershiponline.co.za/articles/cyber-crime-escalates-in-south-africa> [Accessed 2 May 2013].

- Coetzer, P. 2013. *Cyber war becomes reality*. [Online]. Available: <http://www.leadershiponline.co.za/articles/cyber-war-becomes-reality> [Accessed 23 April 2013].
- Creative Commons. 2013. About creative commons. [Online]. Available: <http://creativecommons.org/> [Accessed 6 September 2013].
- Cyberbullying Research Centre. 2013. *Cyberbullying research centre resources*. [Online]. Available: <http://cyberbullying.us/> [Accessed 9 May 2013].
- Cybercitizenship.org. n.d. *What is cyber crime?* [Online]. Available: <http://www.cybercitizenship.org/crime/crime.html> [Accessed 2 May 2013].
- Cybercrime.org. 2013. *Cybercrime Safety & Security guide*. [Online]. Available: <http://cybercrime.org.za/> [Accessed 2 May 2013].
- Debons, A. 1988. *Information Science. An integrated view*. Boston: GK Hall.
- EPR Working Group. 2003. *Extended producer responsibility: a prescription for clean production, pollution prevention and zero waste*. [Online]. Available: <http://www.eprworkinggroup.org/> [Accessed 29 August 2013].
- Erasmus, J. 2009. *E-waste pilot project delivers*. [Online]. Available: <http://www.mediaclubsouthafrica.com/index.php?option=com_content&view=article&id=997:e-waste-260209&catid=45:economynews&Itemid=114> [Accessed 10 August 2013].
- ET. 2013. *Social networking blog.* [Online]. Available: <http://www.ewdisonthen.com/> [Accessed 6 September 2013].
- ExtremeTech. 2013. *Information appliance.* [Online]. Available: <http://www.extremetech.com/> [Accessed 6 September 2013].
- FBI.gov. n.d. *Cyber Crime*. [Online]. Available: http://www.fbi.gov/about-us/investigate/cyber/cyber [Accessed 2 May 2013].
- Friedman, B., Kahn, P., & Borning, A. (Forthcoming). Value Sensitive Design and Information Systems. In: P. Zhang, & D. Galletta. (Eds.) *Human-Computer Interaction in Management Information Systems: Foundations*. M.E. Sharpe, Inc: NY.
- Georgia Tech College. n.d. *Research community drupal server.* [Online]. Available: <https://research.cc.gatech.edu/> [Accessed 6 September 2013].
- Girard, J. & Allison, M. 2008. Information Anxiety: Fact, Fable or Fallacy. *Electronic Journal of Knowledge Management,* 6 (2): 111-124.
- Grolier Inc. 1997. *Academic American encyclopaedia.* Danbury, Conn: Grolier.
- Hall, C. 2013. *NSA exposes cloud computing's weakness*. [Online]. Available: <http://fossforce.com/2013/07/nsa-exposes-cloud-computings-weakness/> [Accessed 29 August 2013].
- Cybercrime.org. 2013. Cybercrime Safety & Security guide. [Online]. Available: <http://cybercrime.org.za/> [Accessed 2 May 2013].
- Haralambos, M. & Holborn, M. 2000. *Sociology. Themes and Perspectives*. 5th ed. HarperCollins: London
- Holmner, M. A. 2008. A critical analysis of information and knowledge societies with specific reference to the interaction between local and global knowledge systems. PhD Thesis.
- Holmner, M. 2011. *E-waste opportunities and challenges from a developing perspective*. [Online]. Available: <http://www.globdev.org/files/Globdev%20e-waste%20Panel.pdf> [Accessed 20 August 2013].

- Hughes, G.J. 2012. *Moral dilemmas*. [Online]. Available: <http://www.thinkingfaith.org/articles/20120919_1.pdf> [Accessed 20 August 2013].
- ICT4D. 2013. *Information and communication technologies for development*. [Online]. Available: <http://www.ict4d.org.uk/> [Accessed 28 August 2013].
- ICTD. 2010. *ICTD London conference*. [Online]. Available: <http://www.ictd2010.org/> [Accessed 24 August 2013].
- IDIO. 2013. *Trust image*. [Online]. Available: <http://www.idioplatform.com/> [Accessed 5 September 2013].
- IISD. 2013. *What is sustainable development*? [Online]. Available: <http://www.iisd.org/sd/#one>. [Accessed 20 August 2013].
- INTERPOL. 2013. *Cybercrime*. [Online]. Available: >http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> [Accessed 2 May 2013].
- Investopedia. 2013. *Definition of accountability*. [Online]. Available: <http://www.investopedia.com/terms/a/accountability.asp> [Accessed 20 August 2013].
- Investopedia. 2013. *Definition of whistleblowing*. [Online]. Available: <http://www.investopedia.com/terms/w/whistleblower.asp> [Accessed 24 August 2013].
- ITGSopedia. 2013. *Digital divide image.* [Online]. Available: <http://itgsopedia.wikispaces.com/> [Accessed 6 September 2013].
- Jaeger, P.T. & Burnett, G. 2005. Information access & exchange among small worlds in a democratic society: The role of policy in shaping information behaviour in the post-9/11United States. *Library Quarterly,* 75(4): 464-495.
- Korhonen, J. 2003. On the ethics of corporate social responsibility: Considering the paradigm of industrial metabolism. *Journal of Business Ethics*. 45: 301-31.
- Lagasse, P. (Ed.) 2001. *The Columbia encyclopaedia.* 6th ed. Columbia University Press: Columbia.
- Letswatchtech. 2013. *Virtue ethics image.* [Online]. Available: <http://letswatchtech.blogspot.com/> [Accessed 5 September 2013].
- London Business School. 2013. *Digital revolution image.* [Online]. Available: <http://bsr.london.edu/> [Accessed 6 September 2013].
- Lor, P.J. & Britz, J.J. 2007. Is a knowledge society possible without freedom of access to information? *Journal of Information Science,* 33(4): 387-397.
- Mason, R.O. 1986. *Four ethical issues of the information age*. [Online]. Available: <http://www.ida.liu.se/~TIMM32/docs/4etical.pdf> [Accessed 26 August 2013].
- Martin, W.J. 1988. *The information society.* Aslib: London.
- Mawson, N. 2013. *IT Web Security*. [Online]. Available: <http://www.itweb.co.za/index.php?option=com_content&view=article&id=63654> [Accessed 2 May 2013].
- McArthur, V. 2008. Real ethics in a virtual world. *CHI 2008 Proceedings, April 5 - April 10* (pp. 3315-3320). Florence: CHI.
- McConnell, T. 2010. Moral Dilemmas. In: *The Stanford Encyclopedia of Philosophy.* Summer 2010 ed. Edward N. Zalta (Ed.). [Online]. Available: <http://plato.stanford.edu/archives/sum2010/entries/moral-dilemmas/> [Accessed 29 June 2013].

- McGilvrey, D. 2008. *Executing data quality projects: ten steps to quality data and trusted information.* Morgan Kaufmann: Burlington, MA.
- *Merriam-Webster Dictionary*. 2013. *Definition of hacker*. [Online]. Available: <http://www.merriam-webster.com/dictionary/hacker> [Accessed 28 July 2013].
- Miceli, M.P. and Near, J.P. 1984. The relationships among beliefs, organisational position and whistleblowing status: a discriminant analysis. *Academy of Management Journal,* 27(4): 687-705.
- Murdock, G. & Golding, P. 1989. Information Poverty and Political Inequality: Citizenship in the Age of Privatized Communications. *Journal of Communication,* 39(3): 180-195.
- Nemours. 2013. *Kidshealth: cyberbullying*. [Online]. Available: <http://kidshealth.org/parent/positive/talk/cyberbullying.html> [Accessed 2 May 2013].
- Nickel, P. 2011. Ethics in e-trust and e-trustworthiness: The case of direct computer-patient interfaces. *Ethics and Information Technology,* 13: 355-363.
- Noelle, K. 2013. *E-trust image.* [Online]. Available: <http://www.kristinnoelle.com/> [Accessed 6 September 2013].
- OCDE. 1996. *The knowledge-based economy.* OECD/GD(96)102: Paris.
- OECD. 2001. *Understanding the digital divide*. [Online]. Available: <http://www.oecd.org/sti/1888451.pdf> [Accessed 20 March 2013].
- OECD. 2013. *OECD guidelines on the protection of privacy and transborder flows of personal data.* [Online]. Available: < http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [Accessed 20 March 2013].
- OECD. N.d. *Extended producer responsibility*. [Online]. Available: <http://www.oecd.org/env/tools-evaluation/extendedproducerresponsibility.htm> [Accessed 23 August 2013].
- Pommeranz, A. *et al.* 2012. Elicitation of situated values: need for tools to help stakeholders and designers to reflect and communicate. *Ethics and Information Technology,* 14: 285-303.
- Prathab, K. and Girish, J. 2006. *E-governance: reaching the unreached*. [Online]. Available: <http://www.it.iitb.ac.in/~prathabk/egovernance/egov.html> [Accessed 20 August 2013].
- Reef IT. 2013. *Information and communication technology image*. [Online]. Available: <http://www.reefit.com.au/> [Accessed 19 May 2013].
- Roberts, J. 2009. The global knowledge economy in question. *Critical perspectives on international business,* 5(4): 285-303.
- Rossouw, D. & van Vuuren, L. 2004. *Business Ethics*. 4th ed. Oxford University Press: Oxford.
- Rouse, M. 2005. *Search SOA DEFINITION cybercitizen*. [Online]. Available: <http://searchsoa.techtarget.com/definition/cybercitizen> [Accessed 3 May 2013].
- Rowley, J. & Hartley, R. 2008. *Organizing knowledge.* 4th ed. Aldershot, Ashgate: England.
- SAFPS. 2008. *The South African fraud prevention service*. [Online]. Available: <http://www.safps.org.za/> [Accessed 29 August 2013].

- SAPS. N.d. *Banking crimes: what is identity theft?* [Online]. Available: <http://www.saps.gov.za/org_profiles/core_function_components/commercial/id_theft.htm> [Accessed 28 August 2013].
- Savage, D. 2006. *Blame, Savage Chickens.* [Online]. Available: <http://www.savagechickens.com/tag/accountability> [Accessed 20 August 2013].
- Scientific American. 2013. *Cyber-warfare image.* [Online]. Available: <http://www.scientificamerican.com/> [Accessed 6 September 2013].
- SKIL. 2003. *What is information literacy?* [Online]. Available: <http://skil.stanford.edu/intro/research.html> [Accessed 28 August 2013].
- Spiegler, I. 2003. Technology and knowledge: bridging a "generation gap". *Information & Management*, 40(6): 533-539.
- Stopcyberbullying.org. n.d. *What is cyberbullying, exactly?* [Online]. Available: <http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html> [Accessed 2 May 2013].
- T/A Initiative. 2013. *What is transparency?* [Online]. Available: <http://www.transparency-initiative.org/about/definitions> [Accessed 20 August 2013].
- Tavakoli, A. A., Keenan, J. P. & Crnjak-Karanovic, B. 2003. Culture and whistleblowing: an empirical study of Croatian and United States managers utilizing Hofstede's cultural dimensions. *Journal of Business Ethics*, 43: 49–64.
- TechTerms. 2013. *Information and communication technology.* [Online]. Available: <http://www.techterms.com/definition/ict> [Accessed 28 August 2013].
- Time. 2013. *China's electronic waste village.* [Online]. Available: <http://content.time.com/time/photogallery/0,29307,1870162_1822148,00.html> [Accessed 23 August 2013].
- Trites, G. 2013. *Information integrity*. [Online]. Available: <http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/asec-information-integrity-white-paper.pdf> [Accessed 28 August 2013].
- Turilli, M., Vaccaro, A. & Taddeo, M. 2010. The Case of Online Trust. *Knowledge, Technology & Policy,* 23: 333-345.
- UCT. 2013. *Information systems.* [Online]. Available: <http://www.commerce.uct.ac.za/informationsystems/> [Accessed 2 September 2013].
- UNESCO. 2010. *E-governance*. [Online]. Available: <http://portal.unesco.org/ci/en/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html> [Accessed 20 July 2013].
- UNESCO. 2013. *Information accessibility*. [Online]. Available: <http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-accessibility/> [Accessed 31 July 2013].
- UNITeS. 2004. *ICT4D can help reduce poverty: UNESCO research report.* [Online]. Available: <http://www.unites.org/n280904.htm> [Accessed 23 August 2013].
- US Justice. n.d. *What are identity theft and identity fraud*. [Online]. Available: <http://www.justice.gov/criminal/fraud/websites/idtheft.html> [Accessed 20 August 2013].

- UTS. 2010. *Guide to writing assignments.* [Online]. Available: <http://www.business.uts.edu.au/teaching/guide/index.html> [Accessed 30 August 2013].
- Velasquez, M.G. 1998. *Business ethics, concepts and cases.* 4th ed. Prentice Hall: New Jersey.
- Williams, A.S. 2010. *Death of advanced recycling fee?* [Online]. Available: <http://wp.istc.illinois.edu/sei/tag/advanced-recycling-fee/> [Accessed 20 August 2013].
- WIPO. 2013. *What is intellectual property?* [Online]. Available: <http://www.wipo.int/about-ip/en/> [Accessed 20 August 2013].
- WiseGeek. 2013. *What is an information appliance?* [Online]. Available: <http://www.wisegeek.com/what-is-an-information-appliance.htm> [Accessed 15 August 2013].
- Wizbowski, R. N.d. *Top 10 ways be a better cyber citizen*. [Online]. Available: <http://www.justaskgemalto.com/us/top-10-ways-be-better-cyber-citizen> [Accessed 3 May 2013].
- WordNet.princeton.edu. N.d. *WordNet Search - 3.1*.[Online]. Available: <http://wordnetweb.princeton.edu/perl/webwn?s=information%20age> [Accessed 3 May 2013].
- WorldBankGroup. 2003. *Lifelong learning in the global knowledge economy: Challenges for developing countries.* World Bank: Washington.
- Wurman, R.S. 1989. *Information Anxiety*. Doubleday: New York.
- WWWMetrics. n.d. The growth of online banking. [Online]. Available: <http://www.wwwmetrics.com/banking.htm> [Accessed 30 August 2013].

Websites used for information/images: All accessed between February 2013 and March 2013

http://wordnetweb.princeton.edu/perl/webwn?s=information%20system

http://www.businessdictionary.com/definition/information-system.html

http://www.commerce.uct.ac.za/informationsystems/

Sources consulted (not cited)

- Brey, P. 2012. Anticipating ethical issues in emerging IT. *Ethics and Information Technology,* 14: 305-317.
- Kaptein, M. & Wempe, J. 2002. *The balanced company: A theory of corporate integrity*. Oxford University Press: Oxford.
- Pieters, W. & Becker, M.J. 2008. Ethics of e-voting, an essay on requirements and values in Internet elections – publication detail uncertain. Received copy from author.
- Scott, J. & Marshall, G. 2005. *Oxford Dictionary of Sociology*. Oxford University Press: Oxford.

- Singer, P. Ed. 1991. *A Companion to Ethics*. Blackwell Publishing.: Oxford.
- Webber, S., & Johnston, B. 2000. Conceptions of information literacy: new perspectives and implications. *Journal of Information Science,* 26(6): 381-397.

A note of thanks

I would like to sincerely thank the following people:

- Ms Erin Hommes for her dedication and commitment to this project, and especially for taking charge of the referencing. Thank you for patiently sharing your Information Science knowledge with me.
- Mr Coetzee Bester for recognising the need for this book and providing the opportunity and guidance for its compilation.
- Prof. M.S. Olivier at the Computer Science Department (UP) for helping me out with some of the concepts in this book like hacking and cracking and the opportunities he has given me for exposure to issues in the ICT field.
- The production team for their input while I was abroad. I appreciate your feedback.
- My friends and family who willingly or unwillingly allowed me to bounce different ideas and formulations off them – thank you!

Candice

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkleiers • Leading Minds • Dikgopolo tša Dihlalefi

African Centre of Excellence for Information Ethics
IT 6-46.1 • Department Information Science • Information Technology Building
University of Pretoria • Private Bag X20 • Hatfield • 0028 • South Africa
Tel: +27 (0)12 420 5218 • E-mail: aceie@up.ac.za

www.up.ac.za/aceie