Social Issues and Professional Practice in IT & Computing

Lecture Notes

Department of Computer Science
University of Cape Town

2019

Contents

Chapter 1

Introduction

A good place to start with this course is to look at the reasons why we should look into social issues and professional practice (SIPP) at all. To facilitate this, we look at a few scenarios, some of which are distinctly within the scope of SIPP, and one that sounds like it, but is not. Hopefully, these typical questions illustrate to you the diverse character of ethical issues, which include, among others, property rights, privacy, free speech, and professional ethics.

After the motivating scenarios and your initial answers to the questions, we take an introductory step toward how to analyse such scenarios systematically. We close this brief introduction with the aims of the course.

1.1 A few motivating scenarios

For each of the following scenarios, you should consider any questionable ethical issues that it brings afore. At this point you may not be able to answer them, but you may be able to detect them, and might have your own opinion. Write down any thoughts you may have and revisit them after each relevant section to see if your opinion has been affected by the material you have learned.

Scenario 1: Should I copy software?

Rajesh invests small amounts on the stock market. Last year he bought and successfully employed a software package to help him with his investments. Recently, he met Fundiswa who was also interested in using the software. Fundiswa borrowed the package, copied it and then returned it. Both vaguely knew that the software was proprietary but did not read up the details. Did Rajesh and Fundiswa do anything wrong, if so what? More generally, try to answer the following related questions:

- Should the software package have been lent?

- When is it justifiable to break the law? Bad law, inappropriate law or if the law is easy to break?

Scenario 2: Should a company mine data?

Consider the case where Tisetso sells hardware and software to over 100 000 customers per year. She has 10 years of experience. As part of the billing process she keeps information on customers. She buys and uses a data mining tool to derive useful information about her client's information such as postal codes, credit card numbers, ID numbers, etc. Most of this information identifies groups and not individuals. She can then use the information to market her wares more efficiently. Is this ethical since customers did not give her the information for this purpose?

- Should the customer be notified?
- Is there a need for establishment of a policy? If so, what should this policy looks like?
- Professional responsibility (professional Ethics): Do professionals have a responsibility to ensure computing serves humanity well?

> **Data mining**
>
> *Data mining* is a process of exploration and analysis of large quantities of data, by automatic or semi-automatic means. This is done in order to discover meaningful patterns and rules. In many cases, the data was not collected primarily for the purpose that the data is used for.

Scenario 3: Freedom of Expression

A student, Gert, posts sex fantasies on a blog (alike blogger.com), called Ling's Journey. The stories are fictional, but Gert named the main character, Ling, after a real student. In the story, he described the rape, torture and murder of Ling. He is also member of a social media newsgroup (alike Facebook), discussing sex acts. An alumnus saw this and reported it to the University as well as to the social media companies. Gert was then arrested and held in custody and the social media companies suspended his account. He was charged with transmitting communication of threat to injure another person, and violating community policies of the respective social media platforms. The charges were eventually dropped and his accounts reinstated. Did Gert really do anything wrong?

- Should self-censorship be enforced. Who decides what is acceptable?
- Is the social media software company responsible for the content on their site?
- Should this data—the blog posts and the social media newsgroup chats—be kept online accessible indefinitely?
- Is there a need for a public policy on freedom of expression on social media, as compared to, say, printed hardcopy books and magazines?

Scenario 4: Professional Responsibility

Khadeejah works for a software development company that develops computer games for children aged 8-14. The latest game that Khadeejah worked on, uses inferential reasoning on social roles and allows players to choose different characters, primarily a macho man or a sexy woman. The game is used mainly by boys. Recently, Khadeejah attended a conference on gender and marginalised groups, where she described the above. The conference delegates discussed the issue of lower participation of women in computing and how to make the industry more attractive to women. At the conference, she also learned that recent research has shown that more diverse teams produce better results, mainly because assumptions are not taken for granted anymore and more ideas are brought to the table.

Back at work, Khadeejah realised that her production team is mostly male.

- Should she refuse to work on this team? Should she ask for the team to be reviewed?
- Do you think that the game will sell as well if a different message was given?
- What is Khadeejah's responsibility, if any, in the team and regarding the games' topics?
- Should the message in games be taken into account?
- Should software development teams be diverse? It justifiable to refuse to work in a team that is not diverse?
- Is diversity, or a lack thereof, a responsibility of the profession?

> **Reasoning**
>
> *Automated reasoning* is a way to infer implicit knowledge from explicitly represented information, using the rules of inference together with a logic in which the information is represented and a set of algorithms that automate and scale up this process on the computer.

Scenario 5: Large Legacy Databases

Another area that we should be considering is the use of computers in social context. This includes the use of a large database by a governmental agency such as home affairs (to keep records of individual's birth, death, address etc), police or the judiciary (for criminal records, fine etc). These agencies have always kept records in paper form long before computers came along.

> **Database**
>
> A *Database* is a structured collection of data stored in a text file such that it facilitates easy manipulation and retrieval of that data by a database management system (the software processing the text file) such as PostgreSQL.

Now these records are being digitised, which also gives the opportunity to link the databases. For instance, to link the Home Affairs database recording foreign nationals to the Primary Education department database, so that illegal immigrants of school-going age can be identified. Now a learner of illegal immigrant parents is detected upon trying to enrol at her local primary school, because of the integration of those databases.

- Should we prohibit integration of those two databases to ensure that children will go to school without fear of deportation?
- What is the implication of keeping large databases by government agencies, ethical or otherwise?
- Does introduction of these database affect free speech? If so how?
- Consider the rights of the individual. Should they be given rights of access to their own data or the ability to change incorrect data? Also consider the impact of incorrect data even if they are changed but not propagated in a timely fashion

1.2 Toward A Framework for Ethical Analysis

Now that you have given initial answers to the questions of each of the scenarios, and perhaps have explored various related topics, you may wonder whether it would always go in all directions, or that there may be some systematic approach to this. There are several mechanisms, in fact.

First, there are some general steps, which also can be used for issues other than SIPP. One commences an ethical analysis by listing all the relevant facts. The stating of facts is, as suggested by Kallman and Grillo [60] "As much as possible, a neutral, logical exercise". Although interpretation is involved in selecting pertinent facts, they are not judged in this step.

Then you should list the stakeholders in the case to determine who is affected by the action being analysed. A judgement must be made as to whether a stakeholder is important enough to be listed. There may also be a number of secondary stakeholders, and including them and their claims might not improve the depth of the case analysis.

As last step, it is necessary to consider the course of action the stakeholders have or are considering taking. This is achieved by asking whether they were or are under an obligation or duty to have done or not have done something. In addition, it is important to evaluate all the reasons that individuals give or may give to justify their actions, that is, failing to fulfil their duty. One way to do this is to ask the question "Does it matter . . . ?" and then consider each of the reasons given in turn to determine which failings are significant and which are trivial.

Having established one or more of the courses of actions for each stakeholder, the principles pertaining to the following four steps should be applied: 1. Guidelines, 2. Ethical Theory, 3. Legal Issues, and then 4. Weigh up the argument rationally.

Second, there may be guidelines, or even strict rules, from the profession that will indicate, at a high level, what is, and is not, acceptable ethically. They are typically called something like (professional) 'code of conduct'.

Professional codes of conduct are some of the formal guidelines that help guide ethical decisions. These are rules that state the principal duties of all professionals. There are a number of such corporate or professional codes that are relevant for the computing and IT professions (Figure 1.1), for example, those drawn up by the:

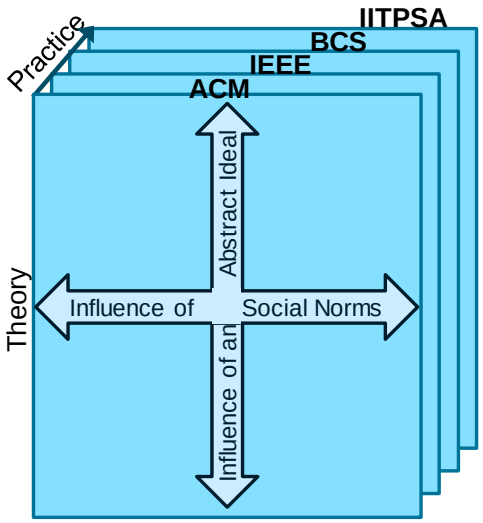

Figure 1.1: Professional Codes

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)
- British Computer Society (BCS)
- Institute of Information Technology Professionals South Africa (IITPSA)
- Ubuntu Leadership Code of Conduct

We shall return to this in Chapter 4 and especially in Section 4.1.1.

1.3 Aims of the Course

While technical issues are central to the computing curriculum, they do not constitute a complete educational program in the field. Students must also be exposed to the larger societal context of computing to develop an understanding of the relevant social, ethical, legal and professional issues. This need to incorporate the study of these non-technical issues into the ACM curriculum was formally recognised in 1991, as can be seen from the following excerpt [113]:

> Undergraduates also need to understand the basic cultural, social, legal, and ethical issues inherent in the discipline of computing. They should understand where the discipline has been, where it is, and where it is heading. They should also understand their individual roles in this process, as well as appreciate the philosophical questions, technical problems, and aesthetic values that play an important part in the development of the discipline.
>
> Students also need to develop the ability to ask serious questions about the social impact of computing and to evaluate proposed answers to those questions. Future practitioners must be able to anticipate the impact of introducing a given product into a given environment. Will that product enhance or degrade the

quality of life? What will the impact be upon individuals, groups, and institutions?

Finally, students need to be aware of the basic legal rights of software and hardware vendors and users, and they also need to appreciate the ethical values that are the basis for those rights. Future practitioners must understand the responsibility that they will bear, and the possible consequences of failure. They must understand their own limitations as well as the limitations of their tools. All practitioners must make a long-term commitment to remaining current in their chosen specialties and in the discipline of computing as a whole.

As technological advances continue to significantly impact the way we live and work, the critical importance of social issues and professional practice continues to increase; new computer-based products and venues pose ever more challenging problems each year. It is our students who must enter the workforce and academia with intentional regard for the identification and resolution of these problems.

Much of this course is concerned with how one decides what to do in situations such as those outlined above. Firstly we must understand the context within which such decisions have to be made. This includes some understanding of our culture and this time and place, that is the concern of Chapter 2. In order to proceed with an analysis of the situations you need a basic theoretical knowledge of ethical arguments and a set of techniques for making logical deductions; this is what we tackle in Chapter 3. We then refine the knowledge to apply to the professions surrounding computing in Chapter 4 and deepen and broaden the scope with intellectual property in the context of software in Chapter 5 and privacy issues in Chapter 6. The topics to be addressed include:

Social Context Computers and the Internet, perhaps more than any other technologies, have transformed society over the past 75 years, with dramatic increases in human productivity; an explosion of options for news, entertainment, and communication; and fundamental breakthroughs in almost every branch of science and engineering. Social Context provides the foundation for all other knowledge units, especially Professional Ethics.

Analytical tools Ethical theories and principles are the foundations of ethical analysis because they are the viewpoints from which guidance can be obtained along the pathway to a decision. Each theory emphasises different points such as predicting the outcome and following one's duties to others in order to reach an ethically guided decision. However, in order for an ethical theory to be useful, the theory must be directed towards a common set of goals. Ethical principles are the common goals that each theory tries to achieve in order to be successful. In order to make decisions a basic ability in ethical argumentation is required.

Professional ethics Computer ethics is a branch of practical philosophy that deals with how computing professionals should make decisions regarding professional and social conduct. There are three primary influences: 1) an individual's own personal code; 2) any informal code of ethical behaviour existing in the workplace; and 3) exposure to formal codes of ethics.

Intellectual Property Intellectual property refers to a range of intangible rights of ownership in an asset such as a software program. Each intellectual property "right" is itself an asset. The law provides different methods for protecting these rights of ownership based on their type. There are essentially four types of intellectual property rights relevant to software: patents, copyrights, trade secrets and trademarks. Each affords a different type of legal protection.

Privacy and Civil Liberties Electronic information sharing highlights the need to balance privacy protections with information access. The ease of digital access to many types of data makes privacy rights and civil liberties more complex, differing among the variety of cultures worldwide.

Chapters 4, 5, and 6 can be done in any preferred order, since they do not strictly depend on each other.

1.4 Exploring SIPP issues

There are regularly articles in the media that are within the realms of social issues and professional practice in IT and computing. The following list is a sampling, guided by 1) being accessible reading in the news (as opposed to academic articles), 2) touching upon a range of diverse topics, 3) they have a local or regional relevance. Read at least one of them and form an opinion about the topic. Then, find a news article relevant to SIPP for IT&Computing that appeared in this calendar year, and post it on the Vula chatroom to share with your classmates.

- Boninger, F., Molnar, A. How companies use school educational software to sell to children. *TimesLive*, 18 August 2016. `http://www.timeslive.co.za/scitech/2016/08/18/How-companies-use-school-educational-software-to-sell-to-children`
- Bejoy, R. Apartheid victims lose 14-year legal battle against Ford and IBM. *GroundUp*, 23 June 2016. `http://www.groundup.org.za/article/apartheid-victims-lose-14-year-legal-batt`
  "IBM, they say, provided database and information storage services that allowed the apartheid government to implement the race-based classification system." Do you think IBM is guilty, or else behaved unethically and therefore ought to have been convicted of a crime (regardless what the law says)? Why? What would you do if you were working for a company that is actively involved applying IT in this way in a country now?
- Epstein, R. How Google could rig the 2016 election. *Politico*, 20 August 2015. `http://www.politico.eu/article/google-2016-election-us-candidates-search/`
  Informal description of a scientific paper on demonstrated effects of search engine manipulation in India. Differences in results can be observed in South Africa as well[1]. Is a search engine company legally allowed to do this? Is it morally ok for a company

[1] see the informal experiment described at `https://keet.wordpress.com/2016/08/13/a-search-engine-browser-and-language-bias-mini-experiment/`, close to South Africa's local elections of 2016.

offering a search engine to manipulate the algorithms in favour of one candidate/party over another, in a democracy? If not, why not?

- Nxumalo, M., No 'killer robot' plans for SANDF. *IOL.co.za*, 3 September 2018. `https://www.iol.co.za/dailynews/news/no-killer-robot-plans-for-sandf-16827299`
  The SA national defence force stated they will not use autonomous weapons systems (AWS), nor does the police intend to use them, for various reasons. Do you agree with the reasons mentioned? Could there be any reasons in favour of using AWS? Are there more reasons against AWS than mentioned in the article? Are there arguments for/against that count especially for South Africa, or Africa in general, with respect to ubuntu?
- Levin, S. New AI can guess whether you're gay or straight from a photograph. *The Guardian*, 8 Sept. 2017. `https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph`
  This news article is an introduction to, and reflection on, the preprint of a scientific paper on the topic. The authors of the paper took some 35326 freely available facial images from dating sites, trained an algorithm on image features (nose shape, grooming style and others), with as result that, given a facial image, it did distinguish correctly 81% of the time between gay and heterosexual men and 71% of cases for women, outperforming human judges. Given that LGTB people are not free of discrimination and prosecution around the world, should this Big Data research have been carried out? While those 35326 people who put their profile picture up might not care to be publicly present, is it acceptable that the images have been used for a different purpose, one that is likely to do more harm than good? Consider the data you have made available online about yourself, would there be any of it that may be useful for such type of data analytics?

Recommended Texts

Manuel Castells preface to the 2010 edition of his "The rise of the network society: The information Age" [21] and in particular pages xvii to xxxi (that is up to and including Section 3 of the preface). This is available online as cited and on Vula. It is largely for historical reasons, to give especially the younger generation an idea of what the perceptions and outlook was like some 10-20 years ago, from the perspective of those 'outside' of IT.

Herman T. Tavani Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing [108]. A fifth edition is now available. All page numbers refer to the fourth edition. The UCT library has a copy of the 1st edition: 174.9004 TAVA

Marianne Talbot Critical Reasoning for Beginners. A series of podcasts making up a six-part course, where you will learn all about arguments, how to identify them, how to evaluate them, and how not to mistake bad arguments for good. Such skills are invaluable if you are concerned about the truth of your beliefs, and the cogency of your arguments [107]. We will address some aspects of it in detail in Chapter 3.

Chapter 2

Social Context

Clearly, the social context we live in now is different from what it was before. For the field of IT and Computing, the current social context where IT is being used and is influencing society is different from the issues it raised even 10 years ago, let alone 20 years (practically no social media) or even 30 years ago (email only for a handful of people, no World Wide Web). Some issues keep reappearing in various incarnations, however. For instance, that automation makes workers redundant and privacy issues. Therefore, we'll first take a bit of a detour with some historical notes so as to better understand the overall social context of IT and society and, to some extent, not have to "reinvent the wheel" of arguments on issues that some technologies raise. Then we proceed to several prominent current developments, such as those in Artificial Intelligence and the changing dynamics of the digital divide.

2.1 A Very Short History of IT

It was during the Second World War, and in its aftermath, that major technological breakthroughs in electronics took place: the first programmable computer and the transistor. Yet it was not until the 1970s that new information technologies became widely diffused, accelerating their synergistic development and converging into a new paradigm. These occurred in several stages of innovation in the three main technological fields: micro-electronics, computers, and telecommunications.

- The transistor made the fast processing of electric impulses in a binary mode possible. This enabled the coding of logic and communication between machines. Semiconductor processing devices—integrated circuits or 'chips'—are now made of millions of transistors.
- The comparatively 'giant leap' forward occurred in 1971 when Intel introduced the 4-bit 4004 microprocessor, that is the computer on a chip, and information-processing power could thus be installed everywhere (where the buyer had enough resources, that is).

- The observation that the number of transistors in an integrated circuit doubles approximately every two years is referred to as Moore's law (named after Gordon Moore). Practically, there was about a doubling of computer processing power every 18-24 months. This will not continue indefinitely due to physical constraints, but combined with developments in parallel processing, computing capacity is still increasing to this day.
- Also, greater miniaturisation, further specialisation, and the decreasing price of increasingly powerful chips made it possible to place them in every machine in our every day life, from dishwashers and microwave ovens to automobiles.
- In the last two decades of the 20th century and the first decade of the 21st, increasing chip power resulted in a dramatic enhancement of micro-computing power. Since the mid-1980s, microcomputers could no longer be conceived of in isolation: they were linked up in networks, with increasing mobility, on the basis of portable computers (and later mobile phones). This, along with the capacity to add memory and processing capacity by sharing computing power in an electronic network, decisively shifted the computer age in the 1990s from centralised data storage and processing in mainframes to networked, interactive computer power-sharing and desktop computers. This change did not only affect the whole technological system, but its social and organisational interactions as well.
- Into the 2010s, storage capacity was so cheap and computing power increased enough, that the time of *Big Data* commenced, where massive amounts of data are analysed algorithmically to find patterns. Such data may have been collected on purpose for it, such as the measurements to compute the black hole image and brain scan image analyses, or 'on the side' initially and then exploited and collected on purpose, such as online user behaviour.

> **Big Data**
>
> *Big Data* has no single definition, but there are either 3 Vs or 5 Vs associated with it: Volume, Velocity, and Variety, to which Veracity, and Value have been added more recently. That is, respectively: the huge amounts of data, the speed at which they are generated, the different types of formats of the data, the trustworthiness of that data, and the money one can make with it.

2.1.1 Networks toward Social Media

This networking capability only became possible because of major developments both in telecommunication and computer networking technologies during the 1970s. But, at the same time, such changes were only made possible by new micro-electronic devices and stepped-up computing capacity. Telecommunications have been revolutionised further by the combination of "node" technologies (electronic switches and routers) and new linkages (transmission technologies). Major advances in opto-electronics (fibre optics and laser transmission) and digital packet transmission technology dramatically broadened the capacity of transmission lines. This opto-electronics-based transmission capacity, together with advanced switching

and routing architectures, such as Transmission Control Protocol/Interconnection Protocol (TCP/IP), are the foundation of the Internet.

In the 1960s there was a call to investigate how computers could be 'connected' to each other in order to create an environment to enhance computer research [85]. The US Department of Defense, through the Advanced Research Projects Agency (ARPA), created the first large computer network in 1969. This resulted in ARPANET, which connected numerous US universities to each other. Eventually, it employed the internet protocol suite (TCP/IP) from 1983. In 1988, South Africa's pioneering email connection to the US (and later an internet node) was set up at Rhodes University [65].

Further still, different forms of utilisation of the radio spectrum (traditional broadcasting, direct satellite broadcasting, microwaves, digital cellular telephony), as well as coaxial cable and fibre optics, offer a diversity and versatility of transmission technologies, which are being adapted to a whole range of uses, and make possible ubiquitous communication between mobile users. Thus, cellular telephony diffused with force all over the world, taking off from the mid-1990s. In 2000, technologies were available for a universal-coverage, personal communication device, only waiting for a number of technical, legal, and business issues to be sorted out before reaching the market.

Each leap and bound in a specific technological field amplifies the effects of related information technologies. For instance, the current smartphone could be seen as "a camera with which you also can call", having changed photo camera technologies along the way. The convergence of all these electronic technologies into the field of interactive communication led to the creation of the current version of the Internet. Time will tell whether it is the most revolutionary technological medium of the Information Age.

The social power and expansion of the internet was at about the same time as the invention of the World Wide Web by Tim Berners-Lee at CERN [22] in 1989. He also decided that the technology should not be proprietary, and this was instrumental in its spread after its release in 1991. It soon superseded the other forms of internet communication (e.g., ftp, Usenet and gopher, which charged licensing fees for the original server implementation).

From the late 1980s there was a growth of commercial providers of networks [128], i.e., the infrastructure. Together with the WWW, this led to a growth of the Web, where now anybody[1] could get connected, and the so-called New Economy of tech companies online, such as offering the ability to buy books online rather than only in the bookshop.

Manuel Castells [20] discusses the information age from those early days with its characteristic optimism, which you may wish to read and in particular the preface to the 2010 edition of his "The rise of the network society: The information Age" [21] (its pages xvii to xxxi (that is, up to and including Section 3 of the preface)).

2.1.2 Data Management toward Big Data

While the progress of connecting devices and the Web is one of the success stories, the other one is data management. The first main step in the early 1970s were the relational databases

[1] well, more precisely, meaning not only the few academics, military, and the frontrunner tech companies, but also other people with resources. We will return to this aspect later in the chapter

Figure 2.1: Left: Lead Apollo software engineer Margaret Hamilton standing next to the code that got the shuttle to the moon in 1969; Right: Katie Bouman, lead computer scientist, with the disks needed to store all the data and her laptop with that first image of a black hole, in 2019 (Source: compilation picture from 9gag).

to store data and manipulate them. This was principally to query the data being stored, such as employee data, library records, and the like.

The early 1990s saw the rise of *data mining*: put all the data in a so-called data warehouse—a time-aware database that is slightly differently structured than a relational database—and test hypotheses on that data using association rules and statistics. For instance, with supermarket data. Let's say, the store manager wants to know that if the cream is put on the shelf next to the strawberries, whether the customers will buy more strawberries and more cream than when they are left in their usual positions (in the fruit isle and dairy isle, respectively). A regular data warehouse for supermarket sales can answer such a question. Likewise, one could test patterns matching the sales data over the year with the weather and discover that, say, lemonade sales go up only if the temperature exceeds 27 degrees Celsius.

The late 2000s saw a third jump in the data management, combining it with even more statistical techniques and algorithms on much more data. Popular techniques are the various *machine learning* algorithms. This data could be collected in different places, hence, have

different formats, is generated fast, and a lot of it is generated. For instance, the News24 website probably records each and every visit, knows it is you (well, your device, at least), how often you visit, how long you stay on the website, on each page, and on each section of the article, where you click and on which page you entered and left. This tracking is done for each visitor, each time. Put differently: it is online user-generated data. This was initially captured with the aim to improve the usability of a site. Now, it's a business model, especially for the sites that provide so-called "free" services: you pay with your personal data, as they can learn so much about the users as to make profit from it.

Machine learning

Machine learning focuses on algorithms to achieve good predictions based on large amounts of training data.

As we shall see later, this has had a huge impact already on *privacy* (see Chapter 6) and its technologies feed into what has been dubbed the *4th industrial revolution*, where lots of data is collected to improve manufacturing and agriculture (see Section 2.3.1). Also, it raises a range of questions, such as to whom the online user-generated data really belongs, whether it is acceptable to use data for a different purpose than it was collected for, the inherent biases that may have been part of the mode of collection that then gets exacerbated by the algorithms, and lack of traceability and explainability of the outcome yet making decisions based on it nonetheless, among other issues [50, 93, 131].

Exercise Try to answer the following questions now, and then revisit them after completing Chapter 3.

- What "free services" are you using? Do you know what those companies do with your data?
- Is it ethical to relegate individual data to being a commodity to be used by a company at their will?
- If you build a tool that requires a user's personal data, would you see any problems in using the data provided, be this for the purpose it was intended for or any possible purpose?
- Some Big Data analysis may outperform humans, e.g., in recognising tumours in brain scan images or in predicting whether a crime suspect is a criminal, yet is still not 100% correct. Should such software be used?
- Consider again Levin's and Boninger's articles from Section 1.4, which are facilitated by Big Data: the former by machine learning 'gay features' from the dating sites' profile pictures and the latter by spyware on the devices and in the software to record usage data for later analysis to track and monitor learners.

2.2 A Time of Transition in Communication and Network Usage

Some people, such as Castells, claim that a new form of society has arisen through a number of major concurrent social, technological, economic, and cultural transformations. This change is at a global scale, but this does not entail that everyone is participating equally in it: many segments of the population of the planet are excluded from the global networks that accumulate knowledge, wealth, and power.

A particular feature of the recent (past 20 years) transformation has been the radical changes in the ways people communicate. The top-down mass media mode has been augmented with, and to some extent replaced by, horizontal digital communication between peers and by what has been called *citizen journalism*. This brought with it a reduced amount of power by the gatekeepers of the mass media and empowered individual citizens to distribute information—or disinformation ('fake news', propaganda, etc.), as the case may be for either mode of communication. In addition, wireless communication can now reach users in most places on earth, albeit at various speeds and various cost.

Also, the changes that have taken place have affected the generations in different ways. For instance, now there are WhatsApp parent groups at schools, or classes have such groups themselves for student communication, and people are used to such instant communication. Compare this with the 'telephone trees' for distribution of information that was functional for many years before: a parent/student was called with a message (e.g., by the teacher), who called two other parents/students and so forth until the class was covered. In between, from about the late 1990s, and to some extent currently still, there are the email lists, and for UCT's course management system, Vula, there are still announcements and chatrooms to distribute information. To guess and reflect, and perhaps discuss with your classmates:

- How do you think that these different modes of communication have affected society?
- Could you argue that one way of communicating is better than the other? If so, how is it 'better', or even 'best'?
- Is there a generational divide regarding the use of digital communication technologies? If so, where about (which year) would you put the before-and-after?

Castells builds his arguments about this new society around the concept of the Network Society because in all key dimensions of social organisation and social practice it is made up of networks. Recent years has seen a lot of research on social network analysis and the understanding of human networks that are mirrored in the social networking sphere, such as cognitive limitations on the number of people one can interact with meaningfully and the notion of 'hubs' (some people seem to be very well connected). Digital networks also have shown to overcome traditional limitations, as it is not bound by national boundaries and has turned into a global system. Recent results also indicate that it may lead to radicalisation of a special interest group, due to the *filter bubble* and *echo chamber* effects.

Filter bubble

The term *filter bubble* refers to that what you see in the search results of

a search engine (or feeds in social media) is determined by your prior interaction, rather than a non-personalised page (or item) rank that is not influenced by the user's prior behaviour.

Echo chamber

The *Echo chamber* is defined[a] as a situation in which people only hear opinions of one type, or opinions that are similar to their own.

[a] https://dictionary.cambridge.org/dictionary/english/echo-chamber

It also must be noted that not everyone participates equally in Castells' "Network Society" for various reasons, notably resource access (device, network, money to buy data) and, e.g., the tooling interface that may not be localised. This has resulted in a new source of global inequality that was already increased by globalisation.

Globalisation

Globalisation[a] is a process of interaction and integration among the people, companies, and governments of different nations, a process driven by international trade and investment and aided by information technology. This process has effects on the environment, on culture, on political systems, on economic development and prosperity, and on human physical well-being in societies around the world.

[a] http://www.globalization101.org/what-is-globalization/

Localisation

Localisation is not the opposite of the term 'Globalisation': it is typically used in the context of localisation of software. This concerns, mainly, the process of translation of terms and pop-up boxes of an application's interface into the language spoken where that software is used, and adapting other features, such as spelling and grammar checking for one's language and autocomplete for words in one's language. One can also localise computer hardware, notably keyboards, adapters, and plugs.

Arguments have been put forward that the Internet and the Web exacerbate inequality as well as that they serve as an equaliser. Both are broad-sweeping claims. What do you think? Can you find data to support that opinion? At the time of writing (2019), the answer probably would be 'it depends'.

2.2.1 Transformation of Communication

Conscious communication is the distinctive feature of humans and the fast-paced changes in communication technologies has intensified in recent years. This has had a profound effect on society.

The Internet is old by computing standards—having started 1969—but it only diffused on a large scale twenty years later, because of several factors:

- regulatory changes & privatisation in the 1990s;
- open source software & open protocols;
- greater bandwidth in telecommunications and switching capacity;
- diffusion of personal computers and local networks;
- user-friendly software programs that made it easy to upload, access, and communicate content: beginning with the World Wide Web server and browser designed by Tim Berners-Lee at CERN in 1990;
- rapidly growing social demand for the networking of everything, arising from both the needs of the business world and the public's desire to build its own communication networks. The number of Internet users on the planet grew from under 40 million in 1995 to about 1.5 billion in 2009 and is estimated at 4.3 billion in March 2019[2].

A few examples of changes in communication are, among others, text-based communication rather than making a phone call, writing an email instead of walking over to a colleague's desk or writing letters, posting holiday pictures on social media rather than sending postcards to friends and family, and being contactable almost anywhere compared to being 'disconnected' when one is travelling.

A lot of research is being conducted to estimate the effects of the changes at an individual and at a societal level. These include effects of reduced human interaction on a person's development and maintenance of social skills, and the pressures of being expected to have to respond fast when contactable anytime, and others.

Democratic Communication

It is not only social media users who understand the power of Internet with respect to voicing community issues and engaging citizens. Democratic governments throughout the world have been using ICTs for improving their services. We all know that democratic countries function well when their government officials understand the needs of their constituents and are able to communicate with them easily. Governments make use of ICT for communication. There are three basic areas where ICT is used, which are access to information, transaction services, and citizen participation [75]. For instance, (1) Statistics South Africa (SSA) provides census data through their website, (2) the South African Revenue Services (SARS) allows the submission of tax returns (among other services) through their eFiling service, and (3) Johannesburg Road Agency (JRA) developed a mobile application that empowers citizens with the ability to be able to report potholes quickly. These three are examples of the 3 categories of benefits of digital governance.

Repressive governments are also aware of the power of the Internet in mobilising community support, especially for a political issue. The Cameroonian government, for instance,

[2] according to `https://www.internetworldstats.com/stats.htm`; estimates and figures aggregated on Wikipedia are slightly lower (`https://en.wikipedia.org/wiki/Global_Internet_usage`)

shut down the Internet after the English-speaking section of the population, which has long felt politically alienated, went on strike [3, 11]. The government had previously tried to shutdown a twitter service that was provided by MTN Cameroon after it was used by citizens to distribute text messages which opposed the president's leadership [18]. Shutdowns of this nature also have an impact on the country's economy [19]. Social media tends to be used in countries which are characterised by strongman leadership to voice the population's discontent with their leaders. It is often blocked for the very same reason. For instance, Yoweri Museveni (President of Uganda since 1986), blocked social media as a "security measure to avert lies ... intended to incite violence and illegal declaration of election results" [34] during the country's last elections.

Dependence of the Internet to express dissent in repressive governments may not be the best approach, since governments (alongside private companies) control the infrastructure (see Table 2.1). This means that governments can prevent people from using the Internet as a medium. There are cases where people have successfully used social media and other Internet services in repressive regimes, as in the case of the Green Movement in Iran [43]. These successes are also accompanied by the improvement of the government's ability to use the Internet against its own citizens. The first benefit that was enjoyed by the Green Movement from social media was that it allowed ordinary citizens to circulate information, thus breaking the regime's monopoly on news distribution [43]. It was also used to mobilise support from expatriates therewith bringing the country's issues to the international stage. This was particularly important because international journalists had been expelled [43]. The government has countered it by placing all ISPs under the control of the state, deploying website blocking technology, limiting Internet speeds, regulating blog writers, using the Internet for the distribution of propaganda, and the formation of an office whose responsibility is to root out and arrest dissenters on the Web [43].

2.2.2 Worldwide Mobile Revolution

Since the 1990s, there has been an explosion of increasing capacity of connectivity and bandwidth in successive generations of mobile phones. This has been the fastest diffusing technology in the history of communication. In 1991 there were about 16 million wireless phone subscriptions in the world. By July 2008, subscriptions had surpassed 3.4 billion and is currently estimated at around 4.5-5 billion mobile phone subscriptions. Such numbers have to be considered with caution before assuming 2/3 of the population has wireless access: some people have more than one subscription (e.g., one SIM card for data and one for airtime) and others share their phone with friends and family.

Studies in China, Latin America, and Africa have shown that poor people give high priority to their communication needs and use a substantial proportion of their meagre budget to fulfil them. In developed countries, the rate of penetration of wireless subscriptions ranges between 82.4% (the US) to 113% (Italy or Spain) and is moving toward saturation point. In countries such as Argentina, there are more mobile phone subscriptions than people.

2.2.3 Digital Convergence

In the 2000s, we have witnessed increasing technological convergence between the Internet, wireless communication, and multiple applications for communicating over wireless networks. This has multiplied the points of access to the Internet. This communication network can exchange anything that can be digitised: texts, audios, videos, software.

> **Digital Convergence**
>
> *Digital Convergence* refers to the fact that we no longer need separate communications channels for different media (such as voice, video, text, etc.) because they are all digitized and can share the same connections and platforms.

There has also been a price reduction in the production of certain electronics thus leading to the ubiquity of certain sensors. This has resulted in what is called the Internet of Things. This the ability to have devices such fridges, stoves, etc and traditional machines such as computers to be able to share data. This means that individuals are able to have 'smart' houses where one can remotely turn their lights on and off, check whether they turned off the stove, etc.

This is particularly important for the developing world because the growth rate of Internet penetration has slowed due to the scarcity of wired telephone lines. In the new model of tele-communications, wireless communication has become the predominant form of communication everywhere, especially in developing countries. Thus, the ability to connect to the Internet from a wireless device is now the critical factor for a new wave of Internet diffusion on the planet. This depends on the building of wireless infrastructure, on new protocols for wireless Internet, and on the spread of advanced broadband capacity.

2.3 Work and Employment Transformed

In globalising the process of production of goods and services, thousands of jobs, particularly in manufacturing, have been eliminated either by automation or by relocation to countries where wages are low. Job creation and the increased education of the labour force has resulted in a sustained improvement of living standards in the industrialised world for a number of years, but is stagnant or on the decline recently (past 10-20 years). This is because the level of compensation for the majority of workers has not followed the growth of productivity and profits. To try to compensate for that, more women have entered the labour force. This decrease of the gender imbalance of the labour force has substantially affected the economic foundations of patriarchalism and capitalism.

In addition, immigration plays a significant role in economies and societies around the world as labour tries to follow global job opportunities. Increased migration is driven by the uneven development of an interdependent world and the networks of connectivity between societies. This leads to a social dynamic concerning multiculturalism and xenophobia as was

seen in the xenophobic riots in South Africa in May 2008, the refugee crisis in Europe, and calls for a border wall between the USA and Mexico, to name but a few examples.

The new job market has seen a parallel growth of highly educated occupations and low-skill jobs, with very different bargaining power in the labour market. This dual structure of the labour market is related to the structural conditions of a knowledge economy growing within the context of a large economy of low-skill services, and it contributes to the growing inequality observed in most societies.

2.3.1 The Fourth Industrial Revolution

Automatisation at the workplace can be beneficial to the workers. For instance, not having to do dangerous work anymore and therewith there will be fewer injuries on the job. It contributes to capital and could make a loss-making company profitable, so that the people who work there can keep their jobs. Yet, automatisation typically has the consequence of firing employees. Also, if all the automatisation in industry continues, it would destroy capitalism, for then it cannot generate the surplus it gets from 'underpaying' workers—i.e., their wages are lower than the value they add with their work—as one cannot underpay a robot as it does not have a wage. So, then there is no profit to be gained, yet capital needs profits to perpetuate itself, so we end up in a contradiction (see [48] for a longer version of this argument). This raises several questions that have no easy answer. Among others:

- What to do with the people who will lose their jobs when more and more tasks are automated?
- Is it ethical to make people redundant due to the software you developed, and are you morally obliged to find alternative gainful employment for the people affected?
- Whose responsibility is it to mitigate this effect, if anyone?
- Do you have an idea how to solve capital's inherent contradiction?

These changes—both the general drive toward automating manual tasks in software, like your online registration process at the university as compared to filling in a paper form and handing it over to a human to process it, and by robots[3]—are expected to very profound in the upcoming years to the extent that it has been dubbed the *Fourth Industrial Revolution*.

The Fourth Industrial Revolution, or, less glamorous, industry 4.0, is said to be driven by a set of technologies, notably including Artificial Intelligence (AI) and the Internet of Things (IoT). The use of IoT in industry generates lots of data, which is then analysed with AI techniques to try to make sense out of the generated data. This combination then is expected to make 'intelligent' cyber-physical systems that can configure themselves based on the input it receives, adjust its configuration accordingly, and, finally, optimise its operations autonomously as well; see Figure 2.2.

[3] the term is used in a broad sense here, and those robots in manufacturing are typically not the humanoid robots you see in the movies.

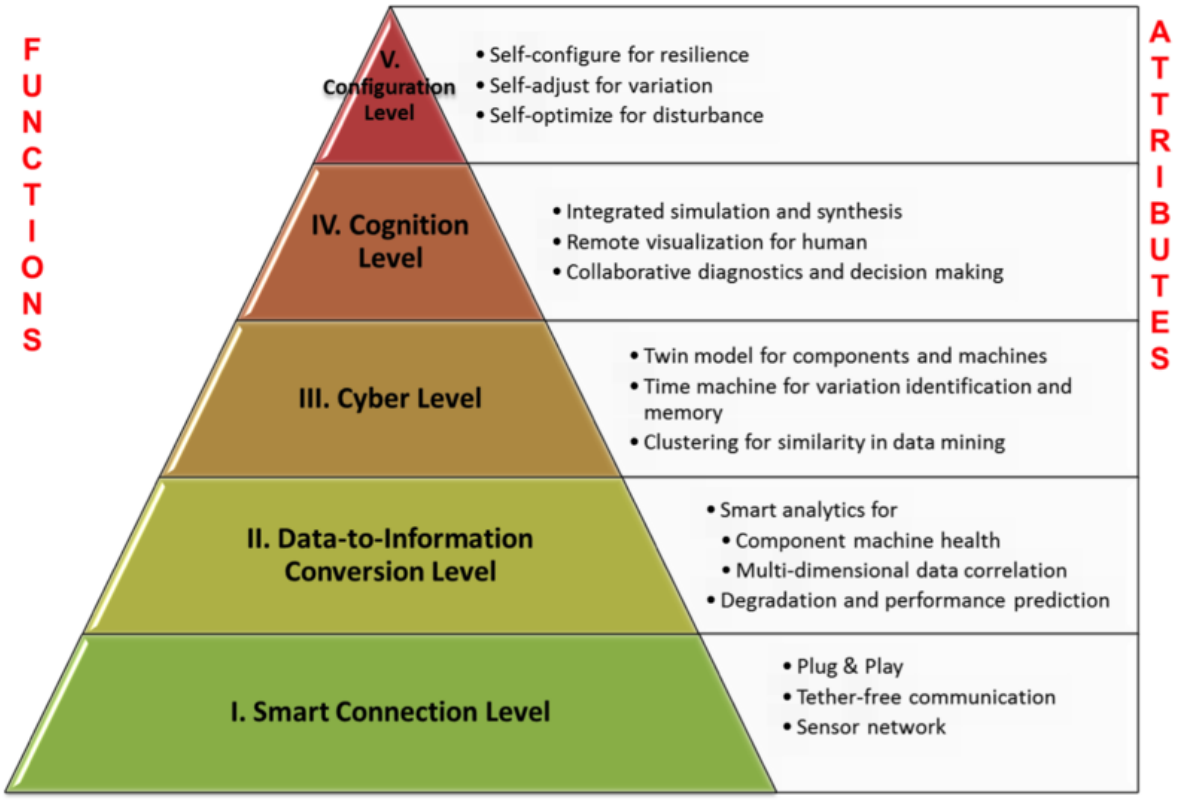

Figure 2.2: A pyramid architecture of a cyber-physical systems-enabled manufacturing system (Source: attributed to [67]).

Artificial Intelligence

Artificial Intelligence is a branch in computer science and IT that concerns the theory and development of computer systems that can carry out tasks that normally requires human intelligence, i.e., it aims to simulate 'intelligent' behaviour in computers. This include subfields that focus on techniques for automated learning and reasoning using, among others, logic, statistics, and language.

Internet of Things

The *Internet of Things* extends the commonly known Internet infrastructure with connectivity of devices that are not regarded as computers but do have embedded electronics so that they can be interacted with remotely, such as sensors, fridges, and other smart home appliances like a security system.

This extends also into agriculture, where it is known as *precision agriculture* to automate farming: sensors collect data about the environment, such as the temperature, humidity, and any pest infestation, and make decisions based on that to manage the plants (e.g., to spray pesticides and to increase or decrease irrigation). Likewise, it is being extended into

smart cities for, among others, better traffic monitoring and pollution control. This would enable, among others, the adjustment of the timing that a traffic light is on green based on the amount of traffic at, or nearing, each particular crossroads.

Overall, this means that a lot of jobs are set to disappear. While this is a fairly common process, it is unclear where new ones will be created, if they required the skills that people have that were made redundant (probably not), and whether that will be a similar amount of jobs that are expected to disappear in the Fourth Industrial Revolution. There are both arguments for excitement and caution regarding the fourth industrial revolution. Whichever way it goes, it is expected to have a major impact on society.

2.3.2 Robots

Robots speak to the imagination and fear that humans have, and have featured prominently in popular culture. The idea of trying to constrain their use can, perhaps, be traced back best to Asimov's laws of robotics, which have been debated widely, extended, and made fun of ever since. Some of the main questions of the technology are: What should robots be allowed to do and what not? Why? How to regulate it?

Three laws of robotics

The *Three laws of robotics* were formulated by science fiction write Isaac Asimov, in an attempt to control humanoid robots in his science fiction novels. They are:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

For instance, they could be deployed in an earthquake zone to search for survivors in the rubble, which may be too dangerous to do for human rescue workers, or in underground mines to save lives. An issue that has arisen is *scope creep* in built-in robot features, or: the robot can do more than it was supposed to be doing. A recent example of this problem is the The Dallas shooting case [40], where a bomb disposal robot was used to kill a suspect, yet one can argue that a bomb disposal a robot does not need shooting capabilities and should not have had that capability in the first place. Also, this robot takes a step in the direction of *autonomous weapons systems*, which will be discussed in Section 2.6.3.

In line with the idea of "let's make robots do things that not enough humans are willing to do", sex robots have been developed. Arguments in favour have been made, as well as against [90]. For instance, it could reduce the number of rapes, as the fantasies could be satisfied with the sex robot, or it may be damaging because of the objectification and especially so for women especially as the sex robots are mostly given a female appearance. This debate has extended further into the question whether anthropomorphic robots should

have rights or not. As Richardson claims, "Extending rights to machines has the potential to reduce the idea of what it means to be human, and to begin to redefine the human as an object, as Aristotle thought of his slaves." and that "Only when confronted with another human can we experience our humanity, our identity, and our mutuality as enshrined by the U.N. Declaration of Human Rights." [90].

Self-driving cars are, in a way, also robots: the driver is replaced by a machine that takes environmental inputs, like where are other elements on the road, knows about the rules of the road, and then has to make a decision. An import philosophical question is what it should do when the choices are always unpleasant. For instance, if the car goes to fast, and the only options are either to drive into three grannies that are crossing the road or swerve aside onto the pavement and hit a playing child that will be killed by the impact, then what should the decision module choose? What if it were the passenger against the grannies? Philosophers have been debating this for decades and haven't come to a conclusion. A few scientists from MIT decided to crowdsource the answer, i.e., to ask many people to answer such questions. In a first experiment, they found out that most people would like cars that sacrifice the passenger for the greater good, but just that those same people wouldn't want to be passengers in such cars and rather see other people drive in them [15]. They then opened up the crowdsourcing app to the world with more scenario—you can play it still[4]—and looked at what happened. After the app had collected 39.61 million clicks (decisions) from 233 countries/dependencies/territories, they analysed the data and it turned out that the moral choices appear to differ by region, i.e., there is a cross-cultural ethical variation. Responses geolocated from South Africa ended up in the 'West' cluster, as did Kenya, Madagascar, Nigeria, Angola, and Tunisia. Whether the clicks recorded are a representative sample is, obviously, a separate question one can argue about. It may, perhaps, be of some surprise to see the results, which are presented in a recent article [102]; its figures 2 is the most interesting, as it disaggregates by attributes like gender, fitness, age, social status, and species.[5] Cautionary notes on the experiment have been voiced as well, so as to not jump to conclusions too soon or to turn that into law already; e.g. [66]. Given the state of self-driving cars technologically at the time of writing and the complete absence of regulation on the matter, cab, minibus taxi, and bus drivers are expected to keep their jobs for another while.

2.3.3 New Jobs

The network society also may be attributed with job generation. The existence of online jobs may seem to give the individual more control over who to work for and when to work. However, it also replicates the existing patterns we see in the manufacturing sector where the opportunities available to certain individuals are limited. In the manufacturing sector, it is known that proletarians, especially in developing countries, are likely to work for low salaries in sweatshops producing material for large companies. Inequalities are replicated, such as the rise of click farms [5] and 'gold farming' [57, 119]. Yet, the Internet also opens

[4]The Moral Machine crowdsourcing app is available at `http://moralmachine.mit.edu/`

[5]scientific news articles and a short video of the main outcomes are available here, respectively: `https://www.nature.com/articles/d41586-018-07135-0` and `https://www.nature.com/articles/d41586-018-07168-5`

gullible people to exploitation. For instance, the Finnish government closed down a service which charged people 1.20€ (about R24) to receive regular SMS texts which it claimed came from Jesus [62].

A recent variant is the so-called "sharing economy", such as Uber and Taxify for a cab ride, where software is used for matchmaking between clients and service providers. Put differently: there is a software platform to support peer-to-peer economic activity, where a percentage of the proceeds goes to the company that developed the software. Societal and economic advantages and disadvantages are widely debated (e.g., [1, 95]) and its effects investigated, including in South Africa [49]. Overall, it does seem to create new jobs, but, as with other areas of the workforce, there is a polarisation of the labour market [6, 14].

Finally, entrepreneurship and innovation continue to thrive on the margins of the corporate sectors of the economy, increasing the numbers of self-employed as technology allows self-reliance in the control of the means of production of knowledge-based services.

2.4 Digital Divide

The adoption of the Internet and other ICTs have not been uniform throughout the world. This inequality is often referred to as the digital divide. By 2009 rates of penetration reached more than 60% in most rich countries and were increasing at a fast pace in countries with emerging economies. By 2018, it is about 90% in Europe and North America, with Africa trailing at 36% yet having seen about 10000% growth since 2000 (see Figure 2.3 for details). Global Internet penetration in 2008 was still at around one-fifth of the world's population and fewer than 10% of Internet users had access to broadband. However, since 2000, the digital divide, measured in terms of access, has been shrinking.

Digital Divide

Digital Divide refers to the disparities in the penetration of the Information Society in terms of access and use of Information and Communications Technologies. It is the gap between those who have access to the Information Society and those who are deprived of such access.

It mirrors and exacerbates existing disparities in society:

- gaps in education (for example, illiteracy)
- disability
- location (rural-urban)
- gender
- race
- income level

The South African Digital Divide grows out of our history of division and historical backlogs for large groups of people.

The ratio between Internet access in OECD and developing countries fell from 80.6:1 in 1997 to 5.8:1 in 2007. In 2005, almost twice as many new Internet users were added in

developing countries as in OECD countries. Thanks to increasing internet access and population numbers in Asia, by now, about half of the global internet users are from Asia. The field that is most directly concerned with addressing issues such as the digital divide is called Information and Communications Technology for Development (ICT4D, ICTD), which draws theories, techniques, methods, and tools for several disciplines, including computer science, information systems, information technology, social science, and economics, and any task-specific domain experts relevant to a project (e.g., water engineers, film & media professionals).

OECD

OECD[a]: The Organisation for Economic Co-operation and Development is an international economic organization of 34 countries, founded in 1961 to stimulate economic progress and world trade. It is a forum of countries describing themselves as committed to democracy and the market economy, providing a platform to compare policy experiences, seeking answers to common problems, identify good practices and coordinate domestic and international policies of its members.

[a] `https://en.wikipedia.org/wiki/Organisation_for_Economic_Co-operation_and_Development`

It would be premature to jump to conclusions about 'the periphery' of the Internet, for there are vast differences among emerging economies as well as on the African continent. For instance[6], China and South Africa had an internet penetration of about 47% of the population in 2015, whereas had India a mere 19% and Nigeria 38% of internet penetration; the percentages for active social media accounts were 46% in China, 22% in South Africa, 9% in India, and 7% in Nigeria, which is thus not proportionate to Internet access.

Also, growth of access is vastly different, both by region of the world and by country. A selection of the data is shown in Figure 2.3, and the latest data can be retrieved from `https://www.internetworldstats.com/stats.htm`.

There is not only a digital divide that mirrors the economic divide in the world, but there are also digital divides within societies. For instance, there is also a generational divide in the use of technologies and, depending on societal norms, a hierarchy in who gets to access a shared computer or phone (e.g, the men first, then women).

If we consider *access* as a binary then we run the risk of seeing a "bipolar societal split" [126, p.6]. This disallows us from seeing the spectrum with respect to access. For instance, consider the three individuals (a) a University of Cape Town lecturer who has a personal computer and a reliable Internet connection, (b) a student from a township, such as Khayelitsha, who has access to an Internet café, and (c) a student who lives in rural area such as Cofimvaba who depends on a family member to print information at work. These three individuals have access to ICT in varying degrees.

[6] the data was sourced from `http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/`.

WORLD INTERNET USAGE AND POPULATION STATISTICS
JUNE 30, 2018 - Update

World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

AFRICA 2018 POPULATION AND INTERNET USERS STATISTICS

AFRICA	Population (2018 Est.)	Internet Users 31-Dec-2000	Internet Users 31-Dec-2017	Penetration (% Population)	Internet Growth % 2000 - 2017	Facebook subscribers 31-Dec-2017
Algeria	42,008,054	50,000	18,580,000	44.2 %	37,060 %	19,000,000
Angola	30,774,205	30,000	5,951,453	19.3 %	19,738 %	3,800,000
Benin	11,458,674	15,000	3,801,758	33.1 %	25,245 %	920,000
Botswana	2,333,201	15,000	923,528	39.6 %	6,057 %	830,000
Burkina Faso	19,751,651	10,000	3,704,265	18.8 %	36,942 %	840,000
Burundi	11,216,450	3,000	617,116	5.5 %	20,470 %	450,000
South Africa	57,398,421	2,400,000	30,815,634	53.7 %	1,184 %	16,000,000
South Sudan	12,919,053	n/a	2,229,963	17.3 %	n/a	180,000
Zimbabwe	16,913,261	50,000	6,796,314	40.2 %	13,492 %	880,000
TOTAL AFRICA	1,287,914,329	4,514,400	453,329,534	35.2 %	9,942 %	177,005,700
Rest of World	6,346,844,099	83.1 %	3,703,602,606	58.4 %	89.1 %	1,942,054,452
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	100.0 %	2,119,060,152

Figure 2.3: Screenshot with some data about internet access. Top: by region in the world; bottom: a selection of countries in Africa (Source: internetworldstats).

This is especially dangerous in the context of rich and poor countries as it creates the notion that rich countries have reached the final destination of information utopia. Furthermore, it may lead to rich countries using poor countries as dumping sites for their old infrastructure, called *trashware*. These countries may do this to avoid the costs associated with responsible disposal of the infrastructure. As highlighted, the simplistic definition of the digital divide has the potential to imply that there are two distinct groups with a gap between them [116]. In such a scenario, one group is motivated to bridge the divide because ICTs may give people the ability to compete economically [116]. The continued exclusion of disabled individuals, and possibly poor countries, may be seen as useful by some to the functioning of current societies. This is because in a "capitalist economy, access needs are determined by the state and extent of the market - the market of production, exchange, con-

sumption, and labor" [116, p.165]. A question that needs to be addressed is whether one believes there should be "equal distribution of resources and opportunities or life chances" [116, p.165] for all individuals, irrespective of country of origin or level of physical ability.

Furthermore, given the huge disparity of Internet use between people over 60 years of age and under 30 years of age, the proportion of Internet users will undoubtedly reach near saturation point in developed countries and increase substantially throughout the world as the older generation joins the ancestors.

There are times where people are not able to directly use ICTs. The barrier is not caused by only financial constraints but rather one's physical abilities. This is the case for individuals who have physical disabilities. Generally, ICTs reportedly have been beneficial to individuals living with disabilities. These benefits range from the ability to get more information about their disability, and improving an individual's communication with others [31]. Unfortunately, the hardware for certain functions such as Braille interface can be expensive [31]. Companies may not consider such individuals as part of their 'intended' audience for their products. This means that there could be a number of websites, machines, etc which may not be suitable for individuals with certain disabilities. In cases such as this, governments tend to intervene. The Americans with Disabilities Act of 1990 can be used, in America, in forcing a company to offer an accessible website [31]. For people with reduced visual abilities, screen readers can be used and, meanwhile, trained as well[7].

2.4.1 Developer Biases, Assumptions, and Values

The designers of software have certain preconceptions about the users of their software, stemming from implicit assumptions or from what came out of the requirements engineering phase of the software development process. Likewise, developers tend to come with their own expectations about the audience for which they are building software. This phenomenon has been studied by Huff and Cooper [54]; the authors studied the impact of a designer's views on educational software for children. They found that designers tend to create gamified tools for boys and learning tools for girls. It is likely that the difference came from an assumption that the educators/designers made based on their experience with teaching children. Fortunately, it was a valid assumption as it has been shown in that survey that children have those preferences [54, p.529]. Unfortunately, there was no difference in the software that designers build for 'general students' and boys whereas there was a difference in the software they designed for girls compared to 'general students'. Thus girls may be disadvantaged when using generic educational software [54].

Sometimes, the problems with our software are not a result of the biases held by the developers. At times, the algorithms designed by developers learn from data it has been given and that data may have been collected with biases and behaviours that are prevalent in that society. This is especially important since machine learning is growing and is using real world data for training. For instance, Microsoft's chatbot, They, learned to tweet racist

[7]For incstance, a recent low-cost solution of training a screen reader to read aloud Description Logic symbols has been described by one of CS@UCT's graduates at `https://people.cs.uct.ac.za/~mkeet/OEbook/ReadingOEbookVI.html`

and anti-Semitic remarks within hours of its deployment on Twitter, and Google's image tagging system once tagged images of black people as gorillas [87].

Some biases are due to a company's intended market for a certain product. For instance, the Eastman Kodak Company, producer of photography products, used Shirley cards to balance skin-tone in still photograph for a long time. The card are named after Shirley, a model who worked for Kodak, and was pictured on the cards [29]. This meant that photos of people who did not have fair skin were not properly balanced. This is the reason that Jean-Luc Godard (circa 1978) did not want to use Kodak film when he was working in Mozambique [29]. Kodak addressed this assumption when two of its biggest clients required the ability in order to photograph dark furniture [101]. The balancing problem had already been solving by Polaroid, however. Its customers, the South African Apartheid government, required the ability to take photographs of individuals who had a dark skin tone. The government used Polaroid's vintage ID-2 cameras for the creation of identity documents as part of its 'dompas' system [101].

There are certain biases that create problems which could be identified and fixed easily in the event that the creators were diverse. For instance, there were reported incidents of the Nikon Coolpix S630 digital camera displaying "Did someone blink?" messages when individuals whose eyes have the epicanthic fold were being photographed [91]. This meant that the message was shown for mostly individuals of Asian heritage even though they were not blinking. A bug of this nature could have been identified in the development process if the creators also included individuals of Asian heritage. It is worth noting that including all groups in the development chain does not guarantee that the resulting products do not suffer from certain biases.

The underrepresentation of certain groups within computer science also has an impact on the industrial culture. Uber[8] is an example of technology company that is struggling with sexism and harassment [68] [69]. The company is not the only company with such problems. An industry culture of this nature does lead to a proportion of women who are already working in the field to change areas. This means that a significant portion of the population may be prevented from participating in computer science and IT.

2.5 Interactive Media and Mass Self-Communication

The World Wide Web offers a means of interactive communication since the "Web 2.0" that started around the 2000s and that made 'posting' content a lot easier than before. A result is that the boundaries between mass media communication and all other forms of communication are blurring. With its diverse range of applications, it is the communication fabric of our lives, for work, for personal connection, for information, for entertainment, for public services, for politics, and for religion.

it is used to access mass media (television, radio, newspapers), and digitised culture or information: films, music, books, and journal articles. It has already transformed television as its reception becomes individualised thanks to a range of streaming services. There has

[8] `https://www.uber.com`

been a similar consequence with print media: users under 30 years of age primarily read on-line. Music listening has been transformed by streaming services as well and the notion of 'leasing' the music, rather than being physical copies (CDs). Business models for such cases are emerging, such as the pay-per-view or monthly subscriptions for TV series and advertisement-free 'premium' for-payment accounts.

Web 2.0 & 3.0

Web 2.0 describes World Wide Web sites that emphasise user-generated content, usability, and interoperability. It is not a technical update but rather refers to an emerging way in which the web is used.

The *Semantic Web* (Web 3.0) is an extension of the web standards by the World Wide Web Consortium (W3C) and refers to W3C's vision of the Web of linked data and knowledge. Semantic Web technologies enable people to create data stores on the Web, build vocabularies, and write rules for handling data.

The developments outlined above have now resulted in a different form of communication: mass self-communication (included in Web 2.0). As people have appropriated new forms of communication, they have built their own systems of mass communication, via SMS, blogs, vlogs, podcasts, wikis, and the like. File sharing and peer-to-peer (p2p) networks make the circulation, mixing, and reformatting of any digitised content possible. For example, YouTube is a video-sharing website where individual users, organisations, companies, and governments can upload their own video content.

This is mass communication, but user-generated content is a very different means of mass communication to what was ever seen before. Unlike traditional broadcast media, anyone can post a video in YouTube, with few restrictions. In most countries everyone is a publisher and there is equal freedom in what is chosen for viewing. A user selects the video she wants to watch and comment on from a huge listing of possibilities. Pressures are of course exercised on free expression on YouTube, particularly legal threats for copyright infringements. There can also be government censorship of content. China blocks access to many foreign websites (they are not "banned"), see [129] for the latest list. China has its own equivalents for many social sites but these are censored. The companies providing these services also may censor material when it is deemed to have violated a company's "community standard". This may lead to problems, for such a standard is formulated by one legal entity in one country, but it is applied across the world where other rules and cultural norms exist. An example of such a problem was the blocking through age restrictions of Youtube videos of reed dancers, because Google did not like bare-breasted women [4].

These new media are self-generated in content, self-directed in emission, and self-selected in reception by many who communicate with many. Castells considered this as a new communication realm, and ultimately a new medium, whose backbone is made of computer networks, whose language is digital, and whose senders are globally distributed and globally interactive.

Horizontal networks of communication built around peoples' initiatives, interests, and desires are multimodal and incorporate many kinds of documents. For example:

Table 2.1: Summary of Internet governance bodies. (Adapted from [32, p.19])

Internet Layer	Layer Function	Governing Body
Infrastructure	It enables the actual connection between network devices	National governments, private telecoms firms
Protocols	These are the languages used by devices to communicate over network	International engineering consortium groups
Applications	These are the tools which allow people to make use of the network	Private commercial software firms, Open-source software developers
Content	This is the actual material that people see, read, listen to, download, watch, and interact with while connected to the network	Private Internet service providers, Hosting companies, Website operators, National and Local governments, Private companies

- Large-scale cooperative projects such as Wikipedia (the open source encyclopaedia)
- Music and films (p2p networks)

The Internet also allows people to share their self-produced content through services such as peer-to-peer services such the DC++, BitTorrent, and others. This means that individuals have greater freedom in distributing contents as they easily distribute their content to their potential audience. There has also been an increase in online streaming services such netflix[9], showmax[10], etc. Individuals, through these services, can now access any show even when the aforementioned show is no longer in season. Furthermore, the users of such services have greater control as what to to watch, and when to watch it, unlike traditional television programming.

2.5.1 Internet Governance

The Internet is governed by a number of organisations to allow a 'decentralised network' run robustly. The overall structure of the governance of the Internet is given in Table 2.1. The groups which are responsible for the protocols used in the Internet include the ICANN, Internet Engineering Task Force, Internet Society, W3C, etc. There are number of telecoms companies which operate in South Africa, these are the mobile providers Telkom Mobile/8ta, MTN, Vodacom, Cell C and Virgin Mobile. Telkom is the largest company (partially owned by the South African government) which provides infrastructure for the Internet.

Net neutrality

Net neutrality refers to the principle that all data packets sent over the Inter-

[9] `https://www.netflix.com/`
[10] `https://www.showmax.com/eng/welcome/za`

net are treated equally.

You may have heard about *Net neutrality*, as it has featured repeatedly in the news over the past five years. It is about all contents being equal on the physical network that constitutes the infrastructure of the internet[11]. It happened to be the case that for the most recent version of one of the internet protocols, IPv6, one has the option to prioritise content. Then one could, for instance, give priority to packets that contain data from Netflix or Youtube over packets that contain data of, say, a GroundUp.co.za news article that wouldn't pay for priority trafficking over the network. Put differently: preferentially allocating bandwidth to who pays more for it. That option was hotly debated for IPv6 standardisation, then included in the standard but not used, then in 2014 asked to be used again (i.e, abandon net neutrality), then after much protest canned and net neutrality reinstated in 2016, then promoted again since the Trump administration in the USA, etc. etc. etc.

One could ask: should we care about what the Federal Communications Committee of the USA decides? After all, we're on another continent. It does matter, as it affects what private telecoms companies can do, and those companies are global companies. It also would affect the response times of websites you are visiting, as most of them are not located on the continent. You may wish to consult the various sources on technical details and socio-political and economic arguments. If you got Tavani's book: see its section 9.9; then there are summaries of technical aspects, such as in [27], and opinion pieces like, e.g., [13], and many more.

2.5.2 Social spaces in the Web

On-line communities have become a fundamental dimension of everyday life and they are growing everywhere, including China and developing countries. In countries with good broadband connections there has been an explosion of interactive computer and video games, today a multi-billion-dollar global industry. The largest on-line game community, World of Warcraft (WOW), which accounts for just over half of the Massively Multiplayer Online Game (MMOG) industry, reached over 10 million active members (over half of which reside in the Asian continent) in 2008.

Social media usage statistics for South Africa are hard to get hold of and publicly available numbers are contested [118]. Commercial surveys are very expensive (over R18K for a report). Table 2.2 has some numbers from 2015. The number of WhatsApp users is not included but likely to be the highest of all.

We can take the South African population in 2016 as 55.91 million people [104]. According to a press release of World Wide Worx [41] we obtain the Table 2.3. They also note that "One of the most significant trends uncovered is that Facebook, with 14-million users, now has 10-million, or 85% of its users, using mobile devices". In another report World Wide Worx [42] estimate that 40% of South Africans use the internet in 2017. The most common use is for communication via social media. Their study also reveals the "stark reality" of the digital divide in South Africa:

[11] a very informal introduction can be accessed at `http://www.savetheinternet.com/net-neutrality-101` and wikipedia-informal at `http://en.wikipedia.org/wiki/Net_neutrality`

Table 2.2: Social Media in South Africa, 2015 [118]

Social platform	% Active	Millions of users
Facebook	22%	11.8
YouTube	13%	7.2
Twitter	12%	6.6
WeChat	9%	5
Mxit	9%	4.9
LinkedIn	7%	3.8
Instagram	2%	1.1
Pinterest	2%	0.84

> The clearest divide is revealed in income disparity. Among adult South Africans earning more than R30 000 a month, Internet penetration is at 82.4 per cent, on a par with overall penetration in many industrialised countries. However, penetration declines rapidly as income declines, falling to 61.3 per cent for those earning between R14 000 and R18 000, 42 per cent for those earning between R3 000 and R6 000, and below 30 per cent for those earning below R2 500 a month.

Furthermore Arthur Goldstuck notes "The research shows that a third of adult Internet users rely on their cellphones as their primary means of access. For low-income users, Internet access requires data costs to be taken off airtime, and those costs remain among the highest in the world".

Table 2.3: Social Media in South Africa, 2016 [41]

Social platform	% Active	Millions of users
Facebook	25%	14
You Tube	16%	8.74
Twitter	14%	7.7
LinkedIn	10%	5.5
Instagram	6%	3.5

The organisation "we are social" [64] publishes world wide data on social media use. Their latest report is dated January 2017. They report, for example, that of a total population of 1 231 million people there are 362 Internet users (29%) and 170 million (14%) social media users. The number of mobile subscriptions stand at 995 million (81%).

Privacy on the communication channels that we use is not guaranteed. Most importantly, even when anonymity is guaranteed with respect to the content of our conversations, the meta-data of the communications could tell malicious actors significant information about us. This is evidenced by the former national security agency (NSA) director's statement, General Michael Hayden, who once said "We kill people based on metadata" [26]. This is important because people tend to share sensitive information in online communications due to their assumption that their conversations are protected [86].

For Castells, the fact is that we no longer distinguish between the virtual online world of

our avatars and the real world of our physical existence. He calls this increasingly hybridised everyday life a "real virtuality".

2.6 ICT for Peace and Warfare

2.6.1 Peace building supported by ICTs

As we have come across "ICT4D", there is also an 'ICT4Peace', which aims to use ICTs for peace building efforts (that may well include ICT4D elements). This is the context of the United Nations definition of *peace building* toward the notion of positive peace as compared to only the absence of physical violence.

Peace building

Peace building[a] includes a "range of measures targeted to reduce the risk of lapsing or relapsing into conflict by strengthening national capacities at all levels for conflict management, and to lay the foundation for sustainable peace and development."

[a] `http://www.unpbf.org/application-guidelines/what-is-peacebuilding/`

Some of the activities categorised under ICT4Peace, are to facilitate communication across divides where physically meeting is too problematic, be that because there is, say, a war zone between refugee camps, or meeting in person might end up in violence but a video conference with some distance as a first step toward negotiated settlement might just work. It may be the recording of facts on the ground (e.g., video recording) and narrating though experiences, such as the Ugandan CD-ROM project[12], or to support the dignity of peoples by recognising their language and localise software accordingly. All these activities require various ICTs.

2.6.2 Building explicit bias into a system

An area within ICTs that can go either way in praxis, is software development: one can use the technologies for the benefit of society or destruction, but also build bias into it. This was already mentioned in Section 2.4.1 for what may be called *implicit bias*. It is a different story for *explicit bias*, where the system's design is driven by political opinion and political agendas [63]. For instance, you are tasked with the development of database to record the incidences of protests in South Africa. How fine-grained should the annotation of events in the database be? Most news outlets simply mention "service delivery protest" but this is a catch-all of a range of issues (number of police, potable water and toilets, bus and taxi routes, delays in RDP housing, lack of delivery of school books, and others), and those categories may change over time as well as split up. One developer may choose a coarse-grained classification 'for easy aggregation' or basically not being interested in whatever it

[12] `https://witness.org/`

is this time, another may prefer a more fine-grained classification of the 'policing' category into numbers on the ground, corruption, and rape cases, and a third involved party may demand that, say, the school books issue be removed because that's politically undesirable to record. What should you do, and build into the system, as software developer when such politically motivated requirements exist?

A related topic that has been touched upon before is the bias in the algorithms, or, more precisely, the data that is fed into the algorithms. One could feed the algorithm past data to learn from it and predict the future. But is the past a good predictor of the future? Do we want the past to be a predictor of the future? If so, it would entail that past mistakes and misconceptions are carried forward into the future. If they were prevalent, then probably not; if they were rare instances, then the noise would be filtered out. An example of the former could be the automatic sentencing of people found guilty of a crime based on past data when there is plenty of evidence it has not been a fair process. An example of the latter could be the automatic classification of brain scans into 'healthy', 'with tumor', and 'signs of Alzheimer' based on many brains scans collected over the past decade.

2.6.3 Destructive ICTs

Thus far, we have seen a multitude of aspects of the social context of ICTs. They tried either to be positive to society, or have some unpleasant 'side effects'. There is, however, also a strand of work in computer science and the deployment of ICTs that has the intention to do harm. At the time of writing, there are two popular topics: *Information Warfare* and *Autonomous Weapons System*.

Information warfare has to do with the 'battle' of information provision, propaganda, and so-called fake news. This has come afore also in the public's attention with the Cambridge Analytica scandal that broke in 2016 and subsequent attempts at damage control: using especially social media to spread disinformation for political gain to influence public opinion and, following that, elections. Of course, there is nothing new to the concept of propaganda, but what is different in this case, is the explicit use of ICTs for nefarious ends as compared to informing the citizenry. It may not directly kill people, but information warfare can be used to manufacture consent to, say, go to war or continue an ongoing war for longer, or spread disinformation about vaccinations that result in a higher incidence of preventable deadly infections.

Autonomous Weapons System

An *Autonomous Weapons System* (AWS), colloquially also called *killer robot*, is a system (hardware+software) that makes decisions autonomously, i.e., without human intervention, for defence or offence purposes, causing physical harm.

As one can have the "self-configuration" etc. in cyber-physical systems to bring a new era in industry (recall Figure 2.2), on could use such theories, methods, and techniques to, say, have a drone self-configure to find the target, self-adjust if that target happens to be moving, and self-optimise toward maximising damage caused by the bomb it drops. This scenario

Figure 2.4: Qinetiq North America's Modular Advanced Armed Robotic System, which is is an "unmanned ground vehicle for reconnaissance, surveillance, and target acquisition missions". (Source: [122]).

is within the arena of (Lethal) Autonomous Weapons Systems (AWS). Such weapons do not have a human that 'presses the red button' to shoot to kill, but the system itself decides what to do based on the data it has gathered and the decision module that is built into the AWS. The fact that AWSs are within reach and, arguably, already have been built, has opened up a can of worms for philosophers, law experts, and ethics boards to chew on (among others, [23, 100, 122]) as well as push-backs from especially AI researchers to not be dragged down in the mud with such application scenarios. The latter included activities such as open letters[13] and stepped-up efforts alike IEEE's "ethically aligned design" vision [110]. Yet, there are people working on realising AWS. One motivating aspect may be a stance such as 'the means (AWS) justifies the ends (e.g,. reduce deaths of soldiers)'. Herewith we solidly enter the arena of moral judgements and ethics, which will receive attention in the next chapter.

2.7 Conclusion

The technological revolution in micro-electronics-based communication technologies and new apps has continued to accelerate, transforming our lives in the way we interact with out another, study, and work. Networks have become the predominant organisational form of every domain of human activity. Globalisation has intensified and diversified. Communication technologies have constructed virtuality as a fundamental dimension of our reality.

[13] The first one being the one presented at the AI flagship conference IJCAI in 2015: `https://futureoflife.org/open-letter-autonomous-weapons/`.

2.8 Revision Questions

1. What is meant by the term "Globalisation"?
2. Is globalisation affecting all peoples equally?
3. Discuss the impact of the trend of globalisation that is being driven by information technology.
4. In what aspect of our lives has the information technology driven revolution had the most impact recently?
5. Castells speaks of a "paradox" of the new economy (with the global networked financial market). What is he referring to?
6. How can the phenomenon of xenophobia be related to globalisation?
7. In which sector does innovation and entrepreneurship still thrive? Why?
8. What technical factor was largely responsible for the sudden and immense growth of the internet? Who was the person who made the essential designs?
9. Which technology has become the preferred platform for bridging the digital divide in the developing world? Why is this?
10. What is meant by digital convergence?
11. Contrast the terms "Web 2.0" and "Semantic Web" (or Web 3.0).
12. Castells uses the term "Mass Self-Communication". What does he mean by this? How is it different from earlier forms of mass communication?
13. What is meant by the "Digital Divide"?
14. Distinguish between two aspects of the Digital Divide.
15. Discuss the consequences of the digital divide for people in developing countries.
16. What do we mean when we speak of leap-frogging in the context of technological advances and the needs of the developing world? Provide an example.
17. What is meant by "Universal Access"?
18. Explain why we might prefer to talk of "Effective Use" rather than "Universal Access"?
19. What sorts of ICTs are appropriate in the developing world? Give two examples and justify by explaining why you think it is the right technology.

Chapter 3

Analytical tools

In this chapter we cover the important ethical tools we require, namely a theoretical grounding (starting in Section 3.1) and an ability to weigh up arguments (from Section 3.6 onward).

Determining what is 'right' is not easy. Declarations like Google's 'Don't be evil' motto are appealing due to their simplicity, however, they are vague. In particular, we often find ourselves in scenarios where our actions need to be guided by principles. Consider the *trolley problem*, as given in Example 3.1. What is considered a good (or bad) decision in situations such as this is different across people. The definition of good and bad is dependent on humans. We live in a world which we share with others and therefore it important that we understand other views and be able to defend our own.

Example 3.1: A version of the trolley problem [35, 12]

> A man is standing by the side of a track when he sees a runaway trolley hurtling toward him: clearly the brakes have failed. Ahead are five people, tied to the track. If the man does nothing, the five will be run over and killed. Luckily he is next to a signal switch: turning this switch will send the out-of-control train down a side track, a spur, just ahead of him. Alas, there's one snag: on the spur he spots one person tied to the track: changing direction will inevitably result n this person being killed. What should he do?

3.1 Computer Ethics

As we saw in Chapter 2, ICT has had a profound impact on our society. Has this transformation also brought about new and unique moral issues? To be able to answer this, we

first have to look into the basic ideas and techniques that we need to address professional issues in computing. and only afterward we will have the machinery to assess ethics of the profession specifically. The former is the topic of this chapter and the latter is deferred to Chapter (4).

We shall use the term "Computer Ethics" to describe the field that examines moral issues pertaining to computing and information technology.

Morality

Morality:[108, p. 5] The etymology (i.e., roots) of morality refers to manners and habits. In this sense, morality is a collection of codes of conduct that are created by the conscience, society or religion. But morality has also a second meaning which emerges from philosophical tradition. According to this tradition, morality is not particular (i.e., specific) but instead is universal. Hence, it provides a sort of ideal code of conduct which has to cope with good and evil. According to this second meaning, which we will retain here, morality is transcendent, and it is inherent to all human beings despite the particular situation. The source of its norms is therefore human reason. It is human reason which is able to exceed the particular, contextual circumstances in order to reveal the spectrum of right and wrong. To act morally is then to act in consideration of this universal spectrum.

Ethics

Ethics[108, p. 5] is the branch of philosophy which studies morality. It is important to understand that the idea that the objects of the study of ethics are therefore the moral rules, the ways in which they are created and justified, and the ways in which they are applied or should be applied. The essential feature of ethics remains in the concept that, besides having to cope with the spectrum of what is right and wrong, it must also deal with the issue of the good life and the search for happiness. This last feature is fundamental because it places ethics inside those particular contexts and concrete dilemmas that are directly experienced by the moral actors who are involved. According to our conception, therefore, ethics is a matter of greater reflection than is morality, in the sense that it tries to analyse the general context of application of the moral code of conduct and to justify its legitimacy.

We could also talk of[1]:

Information ethics to refer to a cluster of ethical concerns regarding the flow of information that is either enhanced or restricted by computer technology.

Internet ethics concerns about ethical issues involving the Internet in particular.

[1]There is also a broader field known as "technoethics"which is concerned with the ethical implications of science and technology.

Cyberethics to broaden the scope beyond individual machines or the concerns of computer professionals.

We shall use computer ethics because computer science is well established term that is not restricted to individual machines nor are its concerns only those of computer professionals.

James Moor defines computer ethics as: "... The analysis of the nature and the social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology." He uses the phrase 'computer technology' so as to take the subject matter of the field broadly to include computers and associated technology: including concerns about software as well as hardware and concerns about networks connecting computers as well as computers themselves [80].

Deborah Johnson defines computer ethics as:

> The study of the ethical questions that arise as a consequence of the development and deployment of computers and computing technologies. It involves two activities. One is identifying and bringing into focus the issues and problems that fall within its scope, raising awareness of the ethical dimension of a particular situation. The second is providing an approach to these issues, a means of advancing our understanding of, and suggesting ways of reaching wise solutions to these problems. [59]

3.2 Ethical theory and concepts

Computer Ethics is *applied ethics* and applied ethics, unlike theoretical ethics, examines "practical" ethical issues. It analyses moral issues from the vantage-point of one or more ethical theories. Ethicists working in fields of applied ethics are more interested in applying ethical theories to the analysis of specific moral problems than in debating the ethical theories themselves [108, p. 14–15].

Our approach is that of professionals seeking ethical guidance. We do however see ourselves as engaged members of our society and as such, for us, Tavani's distinction between professional and philosophical ethics [108, p. 14 ff] is not worth making. It is also clear that we are less interested in descriptive ethics (which report or describe what *is* the case) than in normative inquiries that can tell us what *ought* to be the case.

Descriptive & Normative claims

Descriptive statements: Describe something as a fact (the sky is blue). They can mostly be tested objectively to verify them.

Normative statements: Explores what people ought to do Evaluates arguments, reasons, theories. They are prescriptive and they try to provide an account of why certain behaviours are good/bad or right/wrong

Dialectic

Tavani [108] avoids any discussion of the *dialectical method* (or simply dialectic) as a way of establishing the truth of a philosophical question through rational argument (this is not debate). However it has been a standard technique in Western, Indian, and Buddhist philosophy, since ancient times, for discovering truth through reason and logic in discussion. Contradictory ideas are weighed up and a resolution sought. Such rational analysis consists of:

- establish one or more issues to be analysed.
- for each issue the law and principles presented in agreed guidelines are applied.
- one or more alternative options are presented to be examined rationally and a correct version identified.
- The analysis will disqualify some options to the ethical issue in favour of others.

Inclusive decision-making and participatory meetings are key traditions in rural African communities. Francophone Africans use the term *palaver* to describe how such traditions efficiently institutionalise "communicative action." For instance, Congolese theologian Bénézet Bujo explains [16]: "In seeking a solution for a problem, they share experiences, refer to the entire history of the clan community, and consider the interests of both the living and the dead. The procedure can be time consuming as it is carried on until consensus is achieved". He refers to this as 'spiral thinking' which closely reflects the progress made to resolution in dialectical traditions.

3.2.1 Theoretical Framework

In Figure 3.1 we show three basic approaches to ethics. Virtue ethics deals with character: what would a moral or virtuous person do? Duty based ethics deals with one's duty based on a system of obligations, one of which has been duty to one or more Gods. Consequential ethics focusses on outcomes rather than motives. Good outcomes mean the actions leading to them were good.

Action-based theories focus entirely upon the actions which a person performs, either by their consequences or on how well they accord with obligations.

Consequence-based ethical theories

When actions are judged morally right based upon their consequences, we have *teleological* or consequentialist ethical theory. The Greek *telos*, means "end" or "goal". Consequentialism is a family of theories in which the morally right decision or action is the one with the very best results for people [108, pp. 53–56][98]. This is often summarised as "the ends justify the means". The definition of best with respect to results is defined by the underlying social rules. Correct actions are those that produce the most good or optimise the consequences of choices, whereas wrong actions are those that do not contribute to the good. Three examples of a teleological approach to ethics are Utilitarianism, Egoism and Altruism.

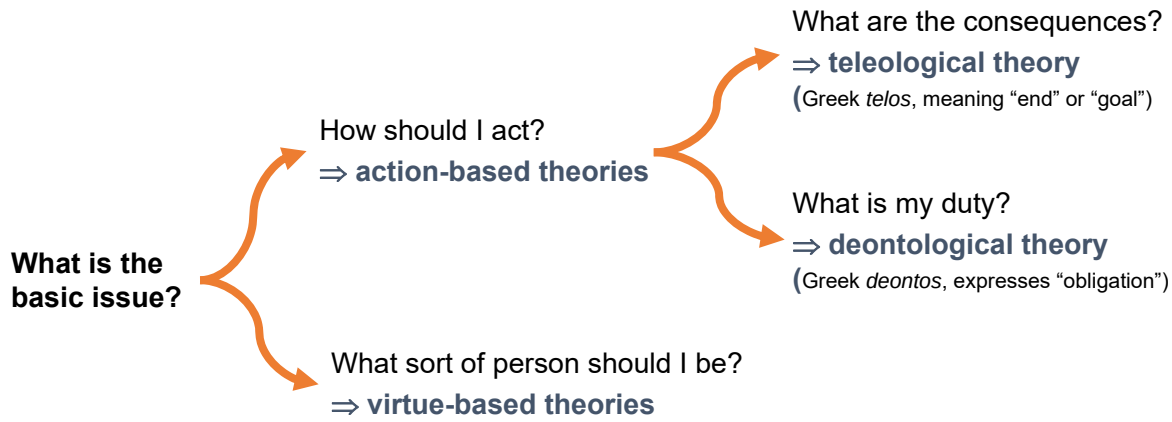

Figure 3.1: Three General Approaches to Ethics: Consequential ethics, Deontological ethics and Virtue ethics.

Utilitarianism The most popular consequential theory is Utilitarianism[2]. The principle of Utilitarianism embodies the notion of operating in the public interest rather than for personal benefit. The principle extracted from this theory determines an action to be right if it maximises benefits over costs for all involved, everyone counting equal.

Ethical Egoism Egoism focuses on self-interest. This ethical principle is used as justification when something is done to further an individual's own (long-term) welfare. Asking the following question can best sum up the principle: "Does the action benefit me, as an individual, in any way?" In the Nichomachaean Ethics Aristotle argues that a man must befriend himself before he can befriend others.

Altruism French philosopher Auguste Comte coined the word altruisme[3]. Altruists see the principle "A decision results in benefit for others, even at a cost to some" as having a justification in evolutionary theory. An action is ethically right if it brings good consequences to others (even at the cost to yourself) Altruists choose to align their well-being with others — so they are happy when others thrive, sad when others are suffering.

Duty-based ethical theories

When actions are judged morally right based upon how well they conform to some set of rules, we have a *deontological* (duty- or obligations-based) ethical theory [108, pp. 56–61]. The Greek *deont*, "that which is binding" expresses duty, that is, actions are essentially right or wrong, without regard to their consequences. Some actions are never justified (ends cannot justify means).

Deontological ethics advocate that there are certain actions which are not morally permissible, irrespective of conditions or context. 'Forbidden' actions often include things such as the killing, rape, and torture of innocent people [98, p.521]. Immanuel Kant (1724–1804) argued that morality must ultimately be grounded in the concept of duty, or obligations that

[2] https://www.utilitarianism.com/
[3] http://www.altruists.org/

humans have to one another, and never in the ethics is based on duty or the obligations owed to people, not the promotion of happiness nor the achievement of desirable consequences. He formulated several versions of a principle he called the "Categorical Imperative"[4]:

1st Principle (1785): "act only in accordance with that maxim through which you can at the same time will that it become a universal law." ⇒ "For an action to be morally valid, the agent – or person performing the act – must not carry out the action unless they believe that, in the same situation, all people should act in the same way."

2nd Principle (1797): "So act that you treat humanity, both in your own person and in the person of every other human being, never merely as a means, but always at the same time as an end" ⇒ killing always wrong, slavery is wrong[5], ...

These ethics are faced with the so-called paradox of deontology. This paradox states that these ethics suffer from the problem of not considering context. For instance, consider the case of the individual who has to kill to prevent more killings. Kant seems to imply that "it would be a crime to lie to a murderer who has asked whether our friend who is pursued by him had taken refuge in our house." [61] since it is our duty to tell the truth always.

Rights-based Ethics

Human rights are the basic entitlements that all people have simply because they are people. The South African constitution [103, Chapter 2] declares:

> This Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.

In Information Technology the rights may be:

- The right to know
- The right to privacy
- The right to property

It seems obvious that every right implies corresponding duties[6] in order to see that right respected, protected, or fulfilled [82]. It seems that these duties are much less emphasised. In the late 1940's when the Universal Declaration of Human Rights was being formulated, Mahatma Gandhi [114, p. 3] said:

> I learnt from my illiterate but wise mother that all rights to be deserved and preserved came from duty well done. Thus the very right to live accrues to us only when we do the duty of citizenship of the world. From this one fundamental statement, perhaps it is easy enough to define the duties of Man and Woman and

[4] Imperative ≡ command, Categorical ≡ no alternative but to adopt (simply because we are rational) ⇒ "Do not act on any principle that cannot be universalized"

[5] Note that a utilitarian justification of slavery could be that the practice of having slaves might result in greater social utility for the majority (e.g., being able to purchase consumer products at a lower price).

[6] Of course human rights could be given a utilitarian justification as well.

> correlate every right to some corresponding duty to be first performed. Every other right can be shown to be a usurpation hardly worth fighting for.

Samuel Moyn rather sarcastically observes (about the USA) that "from their president on down, few Americans seem to believe that a right to be free from torture might translate into a duty to prevent and punish torture." [82].

Exercise. What is the essential difference between Utilitarianism and a duty or rights based ethical approach? Consider:

- In utilitarianism what makes an action right/wrong
  - is outside the action
  - It's the consequences that make it right/wrong
- For deontologists
  - It's the principle inherent in the action If the action done from a sense of duty &
  - If the principle can be universalised
- Then the action is right

Character-based ethical theories

The third major category of ethical theories are *virtue ethics* (or character ethics) [108, pp. 64–66]. It is unlike the categories we have already discussed that focus on duties and results of one's actions. It focuses on the character development of individuals and good character traits. The fundamental principles of virtue ethics were introduced in the writings of Plato and Aristotle nearly 2,500 years ago.

Virtue

A *virtue* is defined by Hursthouse and Pettigrove [55] as follows:

> A virtue is an excellent trait of character. It is a disposition, well entrenched in its possessor —. . . unlike a habit . . . — to notice, expect, value, feel, desire, choose, act, and react in certain characteristic ways. To possess a virtue is to be a certain sort of person with a certain complex mindset. A significant aspect of this mindset is the wholehearted acceptance of a distinctive range of considerations as reasons for action. An honest person cannot be identified simply as one who, for example, practices honest dealing and does not cheat. If such actions are done merely because the agent thinks that honesty is the best policy, or because they fear being caught out, rather than through recognising "To do otherwise would be dishonest" as the relevant reason, they are not the actions of an honest person. An honest person cannot be identified simply as one who, for example, tells the truth because it is the truth, for one can have the virtue of honesty without being tactless or indiscreet. The honest person recognises "That would be a lie" as a strong (though perhaps not overriding) reason for not making cer-

tain statements in certain circumstances, and gives due, but not overriding, weight to "That would be the truth" as a reason for making them.

Virtue ethics does not need to rely on a system of rules. If you ask teleologists or deontologists what to do in a given situation they will try to apply rules. For teleologists the answer depends on the anticipated outcomes, while for deontologists the answer can be determined by using a formal rule to determine your duty. Virtue ethicists ask, "What kind of person should I be?" So the emphasis is on being a moral person, and not simply on understanding how to apply moral rules. The emphasis shifts from learning rules to improving one's character.

Aristotle believed that ethics was something to be lived and practiced, not simply studied. James Moor (in a paper entitled "If Aristotle were a Computing Professional")[81] suggests that virtue ethics can address the lag between ethics and technology. Rule based systems in both ethics and policy will inevitably suffer from not keeping up with the progress and sprawl (in the sense of spreading in every direction) of computer technology. "If we confront new and perplexing policy vacuums with a good character, i.e., a set of dispositions to act virtuously, then we are more likely to fill the vacuums properly than not."[81, p. 16]

3.2.2 Ubuntu

A specially relevant category of virtue ethics is that of *ubuntu*. Ubuntu (from the isiZulu[7]), an African philosophy, emphasises principles of humanness, connectedness and consciousness in human actions and interactions, thereby directly influencing ICT design endeavours. It leads to value-based approaches have heightened awareness of the need to explicitly redefine who is making the design decisions and to explicate what design processes say about users.

Proverb

"umuntu ngumuntu ngabantu" in isZulu

"Motho ke motho ka batho babang" in Setswana

"A person is a person through other persons."

The phrase "A person is a person through other persons" might sound merely descriptive, however for many Africans the phrase also carries an important normative connotation. Personhood, identity and humanness are value-laden concepts. That is, one can be more or less of a person, self or human being, and the more one is, the better [79].

This sense of connectedness is encompassed in the concept of "Ubuntu," which variously means "humanity", "humanness," or "humaneness." It is related to words, aphorisms, and

[7]Cognate terms exist in many Sub-Saharan Niger-Congo B languages, e.g., South Africa: "Ubuntu" isiZulu, "Botho" Sesotho, "Vhuthu" tshiVenda, "Ubuntu" isiXhosa, "Vumunhu" xiTsonga. Elsewhere we have "Vumuntu" shiTsonga and shiTswa (Mozambique); "Unhu" Shona (Zimbabwe); "Ujamaa" Kiswahili (Tanzania); "Bumuntu" kiSukuma and kiHaya, "Utu" Swahili, "Umundu" Kikuyu, "Umuntu" Kimeru (Kenya); "Obuntu" (Uganda), "Bomoto" Bobangi, "Gimumtu" kiKongo (DRC), "Gimuntu" giKwese (Angola) and more.

proverbs in many other African languages. Mbiti, one of the first writers in English on African philosophy, never used the term Ubuntu but explains that a cardinal point in the African view of humanity involves understanding that "I am, because we are; and since we are, therefore I am.' '[76, p. 141] By including all participants' voices in building consensus, Ubuntu reflects a critical discourse. It introduces dimensions that Western discourses do not often associate with community-including a temporality beyond an individual's own life and an accountability to ancestors and descendants. As Mbiti explains: "In traditional life, the individual does not and cannot exist alone except corporately. He owes his existence to other people, including those of past generations and his contemporaries. He is simply part of the whole. The community must therefore make, create, or produce the individual; for the individual depends on the corporate group." [76, p. 106]

Ubuntu as an Ethical Principle

Thaddeus Metz [78] sets himself the task, within African ethics, of stating and justifying a comprehensive, basic norm that is intended to account for what all permissible acts have in common as distinct from impermissible ones. He eventually formulates this as:

> An action is right just insofar as it promotes shared identity among people grounded on good-will; an act is wrong to the extent that it fails to do so and tends to encourage the opposites of division and ill-will [78, p. 338].

To illustrate the implications of Ubuntu for ICT, we rethink the relative identities of the community members and the computer professionals from outside participating in design. Time and again we encounter people in rural African communities explicating the need to act together "as one person" generally, and in relation to ICT projects. Consequently, when we start a new joint design activity we must emphasise facilitation of groups that have *already* established themselves, rather than focusing on bringing individuals together for the undertaking. Furthermore, we need to identify ourselves (as designers from outside) as *part of a wider community* that encompasses designers from inside and outside. Together we derive a communal existence, and we need to acknowledge that it is within this communal existence that "I am" a software engineer. In this situations decisions are arrived at jointly by consensus (see Bujo above, Section 3.2).

The values embedded in Western modes of information exchange, such as "efficiency" and individuals' freedom to express themselves are shaped by media traditions, including writing systems. In contrast, African rural communities (among others) often preserve strong oral traditions, which intertwine with certain values and logics in their local knowledge systems. For instance, speakers frequently personalise and control access to information according to their knowledge about the listener, and this approach contributes to constructing both the speaker's and listener's identities.

Ubuntu and Computer Ethics

As we saw in the previous section, ubuntu seems to argue for greater communal responsibility: this is clearly a guiding principle in the use of Information and Communications Technology for Development (ICT4D — see Section 2.4).

At this stage we make some remarks on the apparent conflict between communitarian values of ubuntu and the individual values of privacy. Ubuntu propagates openness, transparency and surveillance in human interrelationships, which seems to contradict the notion of individual privacy. A full discussion of such privacy issues is left to Chapter 6.

One area in which a tension becomes apparent is in the practice of sharing mobile phones.

Example 3.2: Mobile Phone Sharing in Khayelitsha

> In a study of young mobile phone users in Khayelitsha, South Africa, Walton *et. al* [124] found that phones were extensively shared to the extent that many forms of sharing was not even mentioned since it was unremarkable. A hypothetical scenario where a friend refused to share media on a phone was met with disbelief. A refusal to share phones or media apparently proved that the friendship was faulty and revealed a serious lack of trust. Other interpretations were that the person had something shameful to hide on the phone, was jealous of the friend, or was excessively selfish.
>
> Sharing was not absolute but dynamically changing depending on the relationship to others, allowing secrets (for example, via hidden folders, or trust that a friend would not look at messages) but discreet enough to allow the maintenance of *ukuhlonipha* ("respect"), a concept which encompasses respectful reciprocal relationships towards elders, involving deference, politeness and non-confrontational disagreement.

Exercise. Does Ubuntu have different normative outcomes? Consider what is morally justified in the following [78]:

- to make policy decisions in the face of dissent, as opposed to seeking consensus;
- to make retribution a fundamental and central aim of criminal justice, as opposed to seeking reconciliation;
- to create wealth largely on a competitive basis, as opposed to a cooperative one;
- to distribute wealth largely on the basis of individual rights, as opposed to need.

3.3 Your own rationale for computer ethics

Robert Barger [9] suggested that computer ethics can be grounded in one of four basic philosophies: Idealism, Realism, Pragmatism, or Existentialism (see Figure 3.2. Each person can place themselves in such an ethics space and he developed a questionnaire to uncover your own position, try it! It is available at [10] and the form is available on Vula as well.

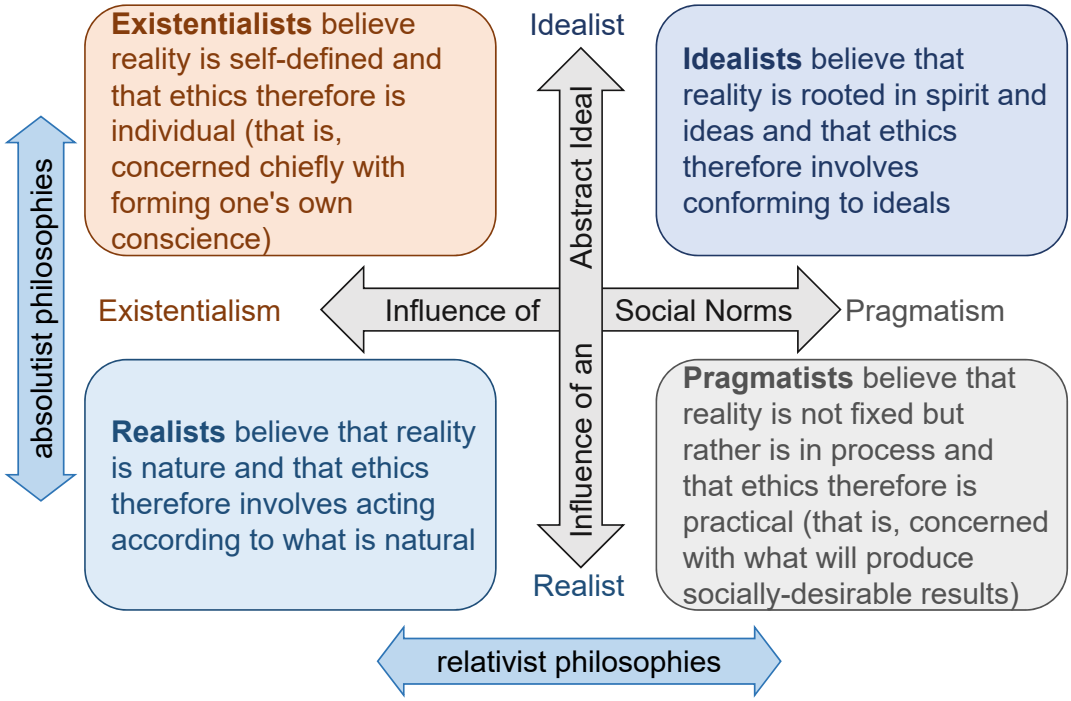

Figure 3.2: Your Ethics Space.

Idealists believe that reality is ideas and that ethics therefore involves conforming to ideals. Realists believe that reality is nature and that ethics therefore involves acting according to what is natural. Pragmatists believe that reality is not fixed but rather is in process and that ethics therefore is practical (that is, concerned with what will produce socially-desirable results). Existentialists believe reality is self-defined and that ethics therefore is individual (that is, concerned chiefly with forming one's own conscience). Idealism and Realism can be considered absolutist philosophies because they are based on something fixed (that is, ideas or nature, respectively). Pragmatism and Existentialism can be considered relativist philosophies because they are based or something relational (that is, society or the individual, respectively).

3.3.1 Assumptions and values

Individuals on a data to day basis make decisions, consciously and unconsciously, based on a set of values. These values are derived from an individual's deeply held moral beliefs. These decisions could be answering question such as the following (adapted from [99])

1. Should Katlego and I live together before marriage?
2. UCT seems tough and irrelevant. Why not drop out and get a better education on my own?
3. What can I do to help improve race relations in Cape Town?

Individuals may provide different answers to the above questions for different reasons. The values continuum strategy presented by Simon et al [99] is great at clarifying diverse

views on the values that individuals may have and may affect a certain decision. The exercise works by mapping each 'view' about a singular issue on a continuum in order the diversity. The work by Simon et al [99] is recommended for strategies of clarifying a group's values which may influence people's decisions. Values is the common term, which has roots in sociology, that refers to the individual's desire to cherish, treasure, and prize certain things [38, p.205]. These values have the following characteristics according to Gaus [38];

1. Valuing, judgements of valuableness, and values provide reasons for actions and choice. They guide choices and enter into deliberation by providing at least a partial ordering of persons, acts, rules, institutions, experiences, objects, etc.
2. We argue about values, judgements of valuableness, and whether certain valuings are correct. We often charge another's values, value judgements, and valuings as wrong, ill-founded, or inappropriate in some way.
3. We often agree to differ about values, their judgements, and valuings. Furthermore, we can also believe that people can disagree and differ on question surrounding value and be able to correctly maintain that neither person is mistaken.
4. Values are often considered to be chosen.
5. valuing is a result of one's emotions and/or also comes from one's desire and volition.

An individual may subscribe to a principle of justice or fairness. In other words, they may believe that if there are goods to be shared then they should be shared justly or equally. An individual may represent all members of the population in an attempt to attract all of them into the field in which they consider to be a 'good' to be shared. Unfortunately, this view is not shared by every individual as evidenced by the work done by Ware and Stuck [125]. It is rare that individuals interrogate the values that lead them to making to such decisions, especially when making decisions about their daily computer related job. This is analogous to the parable that was presented by David Foster Wallace [121] (given in Example 3.3). There are aspects of human life which are crucial but go unnoticed. Our moral judgements are also influenced by the information we have access to in addition to our values [120]. Techniques such as assumption-based planning are effective methods in understanding your assumptions, be they moral or otherwise.

Example 3.3: Parable depicting that some crucial aspects of life may go unnoticed [121].

> There are these two young fish swimming along, and they happen to meet an older fish swimming the other way, who nods at them and says, "Morning, boys. How's the water?" And the two young fish swim on for a bit, and then eventually one of them looks over at the other and goes, "What the hell is water?"

Values: Non-maleficence

The concept of non-maleficence is embodied by the phrase, "above all do no harm". The concept (although not the exact words) first appeared in the Hippocratic Oath for doctors (from the 5th century BCE). We should act in ways that do not inflict evil or cause harm to others. "Don't be evil" was the motto of Google's corporate code of conduct, introduced around 2000 but seemingly dropped subsequently [44].

Values: Informed Consent

Someone must give their agreement freely to do something and they must understand what it is they are agreeing to. This is commonly the requirement for participants in scientific research. For such an assent to have significance, it should be informed, that is, based on accurate information and an understanding of the issues at hand. See for example: "What is informed consent?" from the Department of Health[8]

Values: Ethical Relativism

Ethics is relative: What is right for me might not be right for you. There is (always has been) a good deal of diversity regarding right and wrong. Moral beliefs change over time and in a given society. The social environment plays an important role in shaping moral ideals. All the above are true individually but don't prove (or disprove) that there is a Universal right or wrong.

Values: Golden Rule (ethic of reciprocity)

The Golden Rule is the principle of treating others as you would wish to be treated yourself. It is a maxim of altruism seen in many human religions and human cultures.

For example:

Confucius said in The Analects XV.24 in reply to the question of what would be one word to serve as a rule for ones life "'Is not *reciprocity* such a word? What you do not want done to yourself, do not do to others."[9]

Christianity: "So in everything, do to others what you would have them do to you, for this sums up the Law and the Prophets." Matthew 7:12

Similarly in many other religious and ethical systems[10].

[8] `www.sanctr.gov.za/Whatisinformedconsent/tabid/191/Default.aspx`
[9] Translation by the Chinese Text Project: `http://ctext.org/analects/wei-ling-gong#n1504`
[10] see `www.religioustolerance.org/reciproc.htm`

3.4 Law

When a law tells us to do or not to do something, it implies that a recognised, established authority has decided that the action the law permits or prohibits is of some benefit to society in some way. It often happens that an ethical principle was the basis for any decision regarding this issue before the law was constructed. The fact that the law is often (but not always — consider apartheid laws) grounded in ethical principles makes law a good point for ethical decision making. You can say: "That when we are confronted with an ethical decision, we should first research the law" [60].

In some instances, the law will clearly apply and lead directly to the appropriate ethical conclusion. However, to rely solely on law as a moral guideline is clearly dangerous because four possible states exist in the relationship between ethics and law. The four possible states which depend on whether a specific act is ethical or not ethical, and legal or not legal. Table 3.1 presents these states. This implies that in certain circumstances bad laws exist. Bad laws may bind rules on society that fail to provide moral guidance. Such laws may in some instances excuse a society from fulfilling certain obligations and duties, or allow a society to justify their unethical behaviour. However, beyond any doubt, law and morality do have in common certain key principles and obligations.

Table 3.1: Legality versus Ethicality.

	Legal	**Not Legal**
Ethical	An act that is ethical and legal: e.g., Buying a spreadsheet program and using it to do accounting for clients	An act that is ethical but not legal: e.g., Copying copyrighted software to use only as a backup, even when the copyright agreement specifically prohibits copying for that purpose
Not Ethical	An act that is not ethical but is legal: e.g., Increasing the price of scarce drugs during a disaster situation	An act that is neither ethical nor legal: e.g., Writing and spreading ransomware.

Exercise. Think of four scenarios (which need not be related to computing) that best illustrates each state that exists in the relationship between law and ethics.

3.4.1 Moral and Legal Issues: Policy Vacuum

There are often many points of view to consider when it comes to dealing with ethical issues during periods of rapid change (see also Section 4.1). A good solution walks a fine line in balancing all these factors. However, often another factor against policymakers is time. This results in what is called a *policy vacuum*, i.e., ethical frameworks and laws are lagging behind the innovation. Sometimes it takes a considerable time for the ethical framework to be developed for an innovation as the technology itself evolves so quickly. A policy vacuum is most effectively filled by introduction of appropriate laws, but this takes time. Company or personal policies or social conventions can often effectively fill the gap, while at the same time provide a starting point to framework creation and eventually laws. At other times, it

may lead to exploitation. At the time of writing, there is a world-wide policy vacuum on *Big Data*, and in South Africa and several other African countries, there is also a policy vacuum on, e.g., Facebook's "free basics" option, which has been banned in India (for a debate on the latter, see, e.g., [83, 109]).

As we noted before character-based ethics (such as ubuntu) might be a good fall-back option to help us in situations where action-based ethical theories fall short.

3.5 Scenarios to Consider

Given your background in ethical theory you should now attempt to revisit the scenarios presented in Chapter 1 and apply this to the following scenarios.

Case 1: Anti-Spam or Anti-African?

An organisation dedicated to reducing spam tries to get Internet Service Providers (ISPs) in a Southern African country to stop the spammers by protecting their mail servers[11]. When this effort is unsuccessful, the anti-spam organisation puts the addresses of these ISPs onto its "black list." Many ISPs in the US consult the black list and refuse to accept email from the blacklisted ISPs. This action has two results:

First, the amount of spam received by the typical email user in the United States drops by 5 percent.

Second, tens of thousands of innocent computer users in the Southern African country are unable to send email to friends and business associates in the US.

In the following, analyse the anti-spam organisation from a utilitarian perspective and from a Kantian perspective.

- Who benefits from the anti-spam organization's actions?
- Who is hurt by those actions?
- Did the anti-spam organisation do anything wrong?
- Did the ISPs that refused to accept email from the blacklisted ISPs do anything wrong?
- Did the ISP in the Southern African country do anything wrong?
- Could the anti-spam organisation have achieved its goals through a better course of action?
  What additional information, if any, would help you answer this question?
- Would it make any difference if the amount of spam in the US dropped by 90% as a result of this action?

[11] This scenario is (adapted) from "Ethics for the Information Age", page 50, by Michael J. Quinn, Pearson/Addison Wesley, 2005

Case 2: "The Washingtonienne" Blogger

Jessica Cutler, an assistant to a U.S. Senator, authored a blog under the pseudonym "The Washingtonienne." In May 2004, she was fired when her diary was discovered and published. Up till then, she assumed that it had been viewed by only a few of her fellow "staffers"[12] who were interested in reading about the details of her romantic and sexual life. [108, p. 2].

In her diary, Cutler disclosed that she earned only $25,000 p.a. as a staffer and that most of her living expenses were "thankfully subsidized by a few generous older gentlemen." She also described some details of her sexual relationships with these men, one of whom was married and an official in the George W. Bush administration. She did not use real names but initials that could easily be identified.

In response to the political fallout and the media attention resulting from the publication of her diary:

- Cutler was offered a book contract with a major publisher;
- She was also subsequently sued by one of the men implicated in her blog.

This scenario raises several interesting ethical issues – from anonymity expectations to privacy concerns to free speech, etc. For example, in June 2005, Robert Steinbuch, who says that he is the person Cutler referred to as "RS" on her blog, filed a lawsuit against her, seeking over $75,000 in damages. Steinbuch's complaint describes the case as for "defamation," "invasion of privacy for public revelation of private facts," the "intentional infliction of emotional distress." On May 30, 2007, Cutler filed for bankruptcy in an attempt to protect herself from potential debts.

- Are any ethical issues raised in this scenario, or in blogging cases in general, ethical issues that are unique to computing?

Case 3: Do what your boss asks you to do?

Imagine a software designer, lets call him Wolfgang, who works for Volkswagen in the Diesel Engine design division. His bosses have set very ambitious sales goals for diesel-engined car sales in the US. They realise that their somewhat dated engine cannot meet both US pollution control requirements and customer performance expectations at the same time. So they ask him if he can come up with a fix [24, 52].

He regards this as a fascinating design challenge and eventually comes up with a design that detects: 1. if the car is being subject to a test it then runs such that emissions are legal 2. If the car is on the road it increases performance at the expense of causing illegal pollution.

- Should he have done this?
- What alternatives did he have?
- Are programmers responsible for the social, environmental, moral, . . . , consequences of the code they produce?

[12] "staffers" = Washington D.C. staff assistants (GIYF for more details)

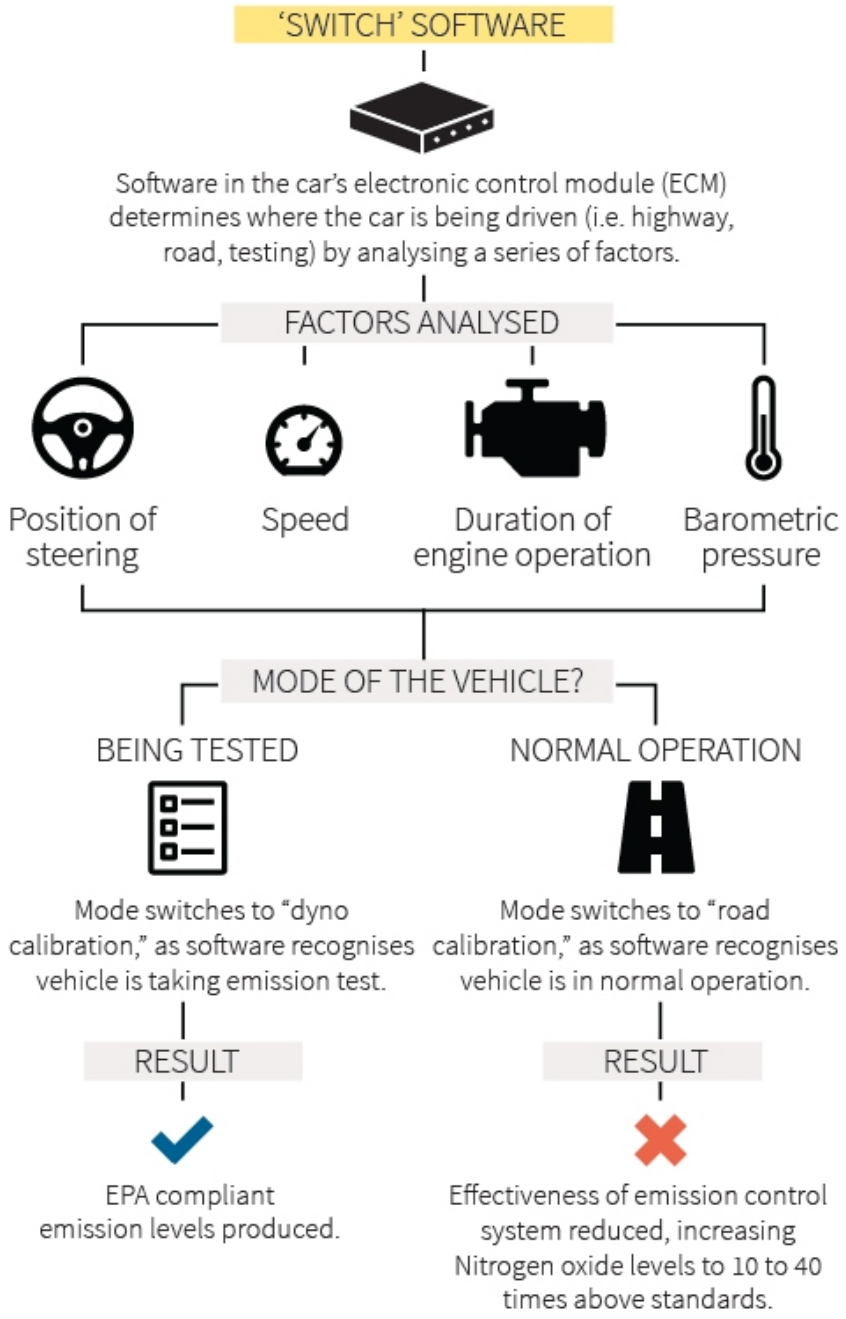

Figure 3.3: Volkswagen's 'defeat device'.
Source: US evironmental protection agency, J. Wang, 22/9/2015 Reuters. `https://www.theautomaticearth.com/tag/defeat-device/`

Now imagine a programmer at VW who is given Wolfgang's design to implement (see Figure 3.3). Lets call her Inge.

- Should she do this?
- If this is wrong, how complicit is she?

This scandal broke in September 2015. In the US it involved ½ million diesel engines and 11 million worldwide. They were clean when tested but once on the road, the cars would pump out as much as 40 times the allowed level of nitrogen oxides. About a third of the company's market value has been wiped out. They were exposed by an NGO "International Council on Clean Transportation"[13].

Case 4: Cellular networks blocked in Parliament

In 12 February 2015 cell phone signals were blocked for Jacob Zuma's state of the nation address (SONA). Signals were being jammed at Parliament in an attempt to prevent negative press, particularly around the disruptions to expected from the Economic Freedom Fighters (EFF). ICT experts have described the proceedings as a "sad day in the country's democracy". Using a signal jammer is illegal in South Africa [117].

"The blocking of the mobile network signals and the use of police officers in the National Assembly were not only illegal but sure signs that the ANC is determined to hold power by force," said ICT expert Adrian Schofield [112].

Africa Analysis MD Dobek Pater said that whilst the blocking of mobile network signals could be construed as an infringement of rights to access information, it is important to remember that this was a specific event at a specific time and there are unlikely to be broader implications for the ICT market or sector [112].

This went to the Western Cape Division of the High Court

- Was such jamming justified?

Majority Verdict Judges Dlodlo and Henney believe the use of a jamming device ahead of the SONA was justified and lawful because signal disruptors are used legitimately to protect officials and dignitaries at such events. They also accept that the use of a signal disruptor for longer than necessary was an only an "unfortunate error" after the individual tasked with switching it off forgot to do so. The separation of powers doctrine is why Parliament should be given the freedom to decide how and what is broadcast "because it clearly affects its functioning and dignity" [74].

[13] http://www.theicct.org/news/epas-notice-violation-clean-air-act-volkswagen-press-statement, http://www.theicct.org/news/press-release-new-icct-study-shows-real-world-exhaust-emissions-modern-diesel-c http://www.theicct.org/real-world-exhaust-emissions-modern-diesel-cars

Minority Verdict Judge Savage's differing view is that in terms of the Constitution Parliament holds no right to dignity because that right is not afforded to institutions of government and that the restrictions on broadcast cannot be justified. Restrictions on broadcast are illogical as members of the public and the media who are present can see and record what happens in the house. Her finding is that the State Security Agency's accidental use of signal jamming as well as Parliament's policy on filming and broadcasting are unconstitutional, unlawful and invalid [74].

- Which verdict do you agree with, if any?

3.6 Critical Reasoning

An opinion is a claim made by an individual. Not all opinions are equal. There are some that are based on evidence and judgment; others are based on feelings only. These should be distinguished from arguments. An *argument* is a collection of *claims* (or *statements* or *sentences*), which are referred to as the *premises*, that are offered as reasons for another claim. The claim being supported is called the *conclusion*. These concepts are used in a branch of philosophy and informal logic, called *critical reasoning*. Informal logic is an attempt to develop a logic that can assess and analyse the arguments that occur in natural language, and of the variety that is "everyday" or "ordinary" language discourse[14]. Critical reasoning tools, especially argument analysis, can help us to resolve many of the disputes in computer ethics [108, Chapter 3] [107].

Examples of good arguments are given in Example 3.4, where the bold sections are the statements offered as the conclusions. We will discuss them afterward.

Example 3.4: Two examples of good arguments.

> It is Monday and it never rains during the week in Cape Town, **so Cape Town has dry weather today**.
>
> (1) An argument about the Cape Town weather.
>
> Muffins contain a lot of sugar. Sugar is unhealthy. **Therefore, eating muffins is unhealthy**.
>
> (2) An argument against eating muffins.

Why are these 'good' arguments? After all, it may well be the case in reality that the day you're reading this is not a Monday and sometimes it does rain on weekdays in Cape Town, especially in winter. Also, one could be finicky about the "sugar" in the second example in Example 3.4: so-called table sugar, which is the kind of sugar that's used to bake muffins, really is unhealthy, but not all sugars are. That they are 'good' arguments has to do with the *structure of the argument*: at least all the premise can be evaluated to true or false, the

[14] `http://plato.stanford.edu/entries/logic-informal/`

sentences are related, and if indeed the premises are true, then the conclusion also holds. We'll dig into this aspect more precisely in the next section.

Examples of bad arguments are shown in Example 3.5

Example 3.5: Two examples of bad arguments.

I am not employed. I have no money. I also want to watch movies. **Websites such as The Pirate Bay (TPB) should be allowed to distribute copyright protected movies.**

(3) An argument against copyright protection for movies.

Software patents block users who have no access to large sums of money for licensing from reusing certain technologies to solve their problems. This stifles innovation. They are open to abuse from patent trolls who sell no products but only make money through suing people who infringe on their patents. **There should be no software patents.**

(4) An argument against software patents.

The arguments in Example 3 and Example 4 both share their respective premises and end with conclusions. Despite the similar structure, these arguments carry different weights. This is due to their respective premises. The strength of an argument can be deduced from its **ARG** conditions: The argument needs to have **A**cceptable premises. The person, to which the argument is addressed, should have good reasons to accept them. They need not know whether they are true in order to accept them, they should only not have good reasons to believe that they are false. The premises should also be **R**elevant to the conclusion, follow a logical order, and support the conclusion. Lastly, the premises should give **G**ood grounds to accept the conclusion as true [46].

Exercise. Now consider the argument in Randy Glasbergen's Cartoon, included here as Figure 3.4. How would you change the argument to make it valid, if possible at all?

Can you rework the bad arguments in Example 3 and Example 4 into a good argument, or are they not salvageable in any way? If not, why not?

Figure 3.4: Penguin logic (source: `www.glasbergen.com/wp-content/gallery/goldie/goldie39.gif`).

3.6.1 Logical Arguments

A logical argument is a set of statements such that:

- One of them is being said to be true (conclusion)
- The other(s) are being offered as reasons for believing the truth of the one (called premises).

Consider the argument:

It is Monday, it always rains on the weekend in Cape Town, so it was raining on the past couple of days.

- List the statements in this argument.
- Which one is the conclusion of the argument?
- Identify the premises.

An assertion is a single statement (possibly complex) that is being stated as a fact. Assertions are either true or false. Which of the following sentences are assertions?

1. It is very dry.
2. Is it very dry?
3. Turn on the water sprinkler!
4. If it is very dry there will be water restrictions.

1 and 4 are assertions (4 is complex but neither its first nor second clause can stand on their own as statements, it is not an argument since the whole sentence is what is being asserted). 2 is interrogative while 3 is imperative [107, Episode 1].

Arguments are neither true nor false, instead arguments are either valid or invalid. A valid argument is one where the conclusion follows from the premises. In addition, if the premises are all true then it is sound (or "good"!).

Deductive Arguments

Deductive arguments are such that if their premises are true then the truth of their conclusion is guaranteed. A deductive argument is either: *valid* (and gives us certainty) or *invalid* and says nothing.

For example:
All penguins are black and white.
That is a penguin
Therefore it is black and white.

For a deductive argument to be *sound*, it must be:

1. *valid* (i.e., the assumed truth of the premises would guarantee the truth of the argument's conclusion);
2. the (valid) argument's premises must also be true in the *actual* world.

A deductive argument is sound if and only if it is valid and all its premises are true.

A *counterexample* is a possible case where the premises in an argument can be imagined to be true while, at the same time, the conclusion could still be false. Note that if a deductive argument is valid, no counterexample is possible. To put it differently: if you can give one counterexample to the argument, then it is invalid.

Inductive Arguments

Inductive arguments are such that the truth of their premises makes the conclusion more probably true. Inductive arguments can be either *weak* or *strong* (worse or better). Thus their conclusions can be slightly more likely, or much more likely.

Example of a strong inductive argument:

> The sun has risen every day for millions and millions of years therefore the sun will rise tomorrow.

Example of a weak inductive argument:

> It has been raining for the past couple of days therefore it will rain today.

Note: Tavani [108, p. 86] is simply wrong to say inductive arguments are invalid. He seems to be basing his argument on Hume: Hume argued that it is impossible to justify inductive reasoning: specifically, that it cannot be justified deductively, so our only option is to justify it inductively. Since this is circular he concluded that our use of induction is unjustifiable. However, Hume then stated that even if induction were proved unreliable, we would still have to rely on it. So Hume advocated a practical scepticism based on common sense, where the inevitability of induction is accepted.

Types of Inductive Arguments

Inductive generalizations: The premise identifies a characteristic of a sample of a population the conclusion and extrapolates that characteristic to the rest of the population.

You evaluate such arguments by considering:

- Is the premise true?
- How large is the sample?
- How representative is the sample?
- Beware of 'informal' heuristics (rules of thumb)
- Is there a counterexample?

Causal generalisations: The premise identifies a correlation between two types of event and the conclusion states that events of the first type cause events of the second type.

You evaluate such arguments by considering:

- Is the premise true?
- How strong is the correlation?
- Does the (putative) causal relation make sense or could it be accidental?
- What causes what?

Arguments from analogy: Arguments from analogy take just one example of something and extrapolate from a character of that example to the character of something *similar* to that thing.

You evaluate such arguments by considering:

- are the two things similar?
- are they similar in respect of something relevant?
- can we find a disanalogy? That is, where the analogy fails in exactly the feature we need to compare

Arguments from authority: take one person or group of persons who are, or are assumed to be, right about some things, and extrapolate to the claim they are right about other things.

You evaluate such arguments by considering:

- who exactly is the source of information?
- is this source qualified in the appropriate area?
- is the source impartial in respect of this claim?
- do other experts make other claims?

The Standard Form and Evaluating Arguments

If we write arguments out in a standard form it enables us to add suppressed premises, us to eliminate cross references, irrelevancies and inconsistent terms. In general it makes it much easier to evaluate arguments [108, pp. 76–78] [107, Episode 3].

$$\begin{array}{ll} Premise_1 & \\ \ldots & optional \\ \ldots & optional \\ Premise_N & optional \\ \hline Conclusion & \end{array}$$

A valid argument is valid solely by virtue of its logical form, not its content. An example of a valid logical form is:

$$\begin{array}{ll} Premise_1 & \text{Every A is a B} \\ Premise_2 & \text{C is an A} \\ \hline Conclusion & \text{C is a B} \end{array}$$

No matter which values are substituted for A, B, and C, the argument in this form is always valid.

A common form of valid argument is *modus ponens* (implication elimination):

$Premise_1$	A implies B
$Premise_2$	A is true
$\overline{Conclusion}$	B is true

To start analyzing an argument you first convert it to standard form [107, Episode 3][108, pp. 89–91].

1. identify the conclusion of the argument;
2. identify each of the premises;
3. add suppressed (assumed) premises;
4. remove irrelevancies;
5. remove inconsistent terms;
6. remove cross-references.

At this stage *do not* evaluate the argument.

Now check the reasoning strength.

For a deductive argument, see whether it is *valid* or *invalid*. So assume the premises to be true, and ask yourself whether the conclusion must also be true when those premises are assumed true. Once you have done that then see if the argument is sound, that is, are the premises true in the actual world?

For an inductive argument, see if it is *weak* or *strong*. (See above for: inductive generalisations and causal generalisations; arguments from analogy and authority.)

Is in any of the cases a counterexample to the argument possible? That is an easy way to disprove an argument.

Now make an overall assessment. Describe the argument's strength of reasoning in conjunction with the truth conditions of the argument's premises. For example is the argument:

- deductive and sound?
- inductive with all true premises?
- inductive with some false premises?
- fallacious with a mixture of true and false premises?
- ... ?

Remember that an inductive argument with premises that are all true is useful while a valid argument with one or more false premises says nothing.

3.6.2 Fallacies

A fallacy is not a false statement but *faulty reasoning* [108, pp. 91–98] [107, Episode 6][70]. We have already seen that it is possible for an argument to contain all true statements (including a true conclusion) and still be (logically) fallacious. There are very many kinds of (informal) fallacies. In particular we are going to look at fallacies of: 1. relevance; 2. vacuity; 3. clarity.

Fallacies of relevance

Non-sequitur: Citing in support of a conclusion something that is true but irrelevant: 1. Bill lives in a large building, therefore his apartment is large; 2. Every year many people are supported through life by their religious beliefs, so their religious beliefs must be true.

Ad hominem: Attacking the person making the argument rather than the argument that is made: How can we take seriously a position regarding the future of our national defense that has been opposed by Senator X, who has been arrested for drunken driving and who has been involved in extramarital affairs?

Pointing out someone's vested interests is an *ad hominem* attack and it is not the same as an ad hominem fallacy. So if someone's research is paid for by the tobacco industry then it is legitimate to attack their right to speak (impartially) on the benefits of cigarette smoking. Of course it does not mean that their arguments are *necessarily* wrong.

Fallacies of vacuity

Circular arguments: Citing in support of a conclusion that very conclusion. In a circular argument the conclusion *is* one of the premises.

Begging the question: Citing in support of a conclusion a premise that assumes the conclusion.

Some examples of begging the question:

It is always wrong to murder human beings
Capital punishment involves murdering human beings
Capital punishment is wrong

"Murder" is given the implication of wrongful killing, thus saying capital punishment is murder begs the question of whether it is wrong or not.

Object-oriented programming (OOP) languages are superior to non-structured programming languages because OOP languages are structured:

OOP languages are structured languages
Object-oriented programming languages are superior to non-structured programming languages

Clearly this offers no argument to establish the superiority of structured languages.

Fallacies of clarity

Fallacy of the heap: vagueness. For example:

> If you have only ten cents you are not rich
> If you are not rich and I give you ten cents then you still won't be rich
> It doesn't matter how many cents I give you, you won't be rich

Slippery slopes: misusing borderline cases. A slippery slope attempts to discredit a proposition by arguing that its acceptance will undoubtedly lead to a sequence of events, one or more of which are undesirable. Though it may be the case that the sequence of events may happen, each transition occurring with some probability, this type of argument assumes that all transitions are inevitable, all the while providing no evidence in support of that. The fallacy plays on the fears of an audience and is related to a number of other fallacies, such as the appeal to fear, the false dilemma and the argument from consequences. For example: X could possibly be abused; therefore, we should not allow X.

Another example:

> We should not continue to allow computer manufacturers to build computer systems that include CD burners. If we allow them to do so, young users will burn copies of copyrighted music illegally. If the rate of unauthorized copying of music continues, recording artists will lose more money. If they lose more money, the entire music industry could be in jeopardy. If the music industry in America declines, the entire US economy will suffer. So, we must prohibit computer manufacturers from providing CD burners as part of the computer systems they build.

Equivocation: trading on ambiguity. For example:

> A feather is light
> What is light cannot be dark
> Therefore, a feather cannot be dark

Straw man: The straw man fallacy is when you misrepresent someone else's position so that it can be attacked more easily, then knock down that misrepresented position, then conclude that the original position has been demolished. It's a fallacy because it fails to deal with the actual arguments that have been made.

For example, contrasting of a new idea with some impossibly bad alternative, to put the new idea in a favourable light. Contrasts should be between the new and the current, not the new and the fictitious.

> Query languages have changed over the years. For the first database systems there were no query languages and records were retrieved with programs. Before then data was kept in filing cabinets and indexes were printed on paper. Records were retrieved by getting them from the cabinets and queries were verbal, which led to many mistakes being made. Such mistakes are impossible with new query languages like QIL.

Red herring: This fallacy is committed when someone introduces irrelevant material to the issue being discussed, so that everyone else's attention is diverted away from the points made, towards a different conclusion.

Arguments cannot easily be placed in the described conditions. Furthermore, the way we counter arguments can also be faulty. The problems range from emotive language to the faulty premises. For instance, one can use biased language when stating the premises, defenders of Apartheid in South Africa referred to it as 'separate development' when making their arguments, and anti-abortion activists in the United States have referred to abortion as "baby killing" when making their arguments. Individuals can also make so-called witch hunt arguments [123]. These arguments have the following ten signs: 1. pressuring social forces; 2. stigmatization; 3. climate of fear; 4. resemblance to a fair trial; 5. use of simulated evidence; 6. simulated expert testimony; 7. non-falsifiability characteristic of evidence; 8. reversal of polarity; 9. non-openness; and 10. use of a loaded question.

The witch hunt, as characterised by these criteria, is shown to function as a negative normative structure for evaluating argumentation used in particular cases.

3.7 Critical Reasoning Exercises

In this section you will be asked to analyse arguments. It is very often best to put the argument in a standard form before attempting further analysis even if you are not explicitly asked to do this.

The exercises from 3.7.1 to 3.7.5 are from "Critical Reasoning for Beginners"[107]. They are actually discussed in class by Dr. Talbot. The times are the points in the video where they are discussed. In Section 3.7.6 the questions are from various sources.

Please practice answering those questions! Answers to Section 3.7.6 will be provided on Vula. Do not even look at answers until you have tried the questions. No practice == no learning.

3.7.1 The Nature of Arguments

Which of these sets of sentences are arguments?

1. Towards lunchtime clouds formed and the sky blackened. Then the storm broke.
2. Since Manchester is north of Oxford and Edinburgh is north of Manchester, Edinburgh is north of Oxford.
3. Witches float because witches are made of wood and wood floats.
4. Since Jesse James left town, taking his gang with him, things have been a lot quieter.

Answers from Video [107, Episode 01: 22:45]

One of these is a good argument, one bad,

Argument One: If it is Monday the lecture will finish at 3.30
It is Monday
Therefore the lecture will finish at 3.30

Argument Two: If it is Monday the lecture will finish at 3.30
The lecture will finish at 3.30
Therefore it is Monday

Answers from Video [107, Episode 01: 1:00:55]

3.7.2 Different Types of Arguments

Can you say which arguments are deductive and which inductive:

1. The sun is coming out so the rain should stop soon.
2. If Jane is at the party John won't be. Jane is at the party, therefore John won't be.
3. The house is a mess therefore Lucy must be home
4. Either he's in the bathroom or the bedroom. He's not in the bathroom, so he must be in the bedroom.
5. The dog would have barked if it saw a stranger. It didn't bark, so it didn't see a stranger.
6. No-one in Paris understands me, so my French must be rotten, or the Parisians are stupid.

Answers from Video [107, Episode 02: 21:03]

3.7.3 Setting out Arguments Logic Book Style

Analyse these arguments:

1. Since Manchester is north of Oxford and Edinburgh is north of Manchester, Edinburgh is north of Oxford
2. Witches float because witches are made of wood and wood floats

Answers from Video [107, Episode 03: 10:14]

Identify all the premises of this argument (don't forget there might be a suppressed premise):

> Socialism did not provide the incentives needed for a prosperous economy.
> Conclusion: Socialism was doomed to failure

Answers from Video [107, Episode 03: 21:47]

> Since many newly emerging nations do not have the capital resources necessary for sustained growth they will continue to need help from industrial nations

Answers from Video [107, Episode 03: 26:15]

3.7.4 What is a Good Argument? Validity and Truth

Analyse if the following is a good argument:

> 60% of the voters sampled said they would vote for Mr. Many-Promise.
> Therefore Mr. Many-Promise is likely to win.

Answers from Video [107, Episode 04: 07:45]

You need not consider the issue of all the questions that to be asked in detail.

Arguments from analogy

> The universe is like a pocket-watch
> Pocket watches have designers
> Therefore the universe must have a designer

Answers from Video [107, Episode 04: 43:35]

3.7.5 Evaluating Arguments

Could this argument be valid?

> 2 + 2 = 5
> grass is green

Answers from Video [107, Episode 05: 29:50]

> grass is green
> ---
> 2 + 2 = 4

Answers from Video [107, Episode 05: 36:35]

Explain why these are non-sequitur

1. Bill lives in a large building, therefore his apartment is large.
2. Every year many people are supported through life by their religious beliefs, so their religious beliefs must be true.

Answers from Video [107, Episode 06: 13:29]

Explain the circles or the question-begging premises in each of the following arguments:

1. Intoxicating beverages should be banned because they make people drunk
2. We have to accept change because without change there is no progress
3. The voting age should be lowered to 16 because 16 year olds are mature enough to vote

Answers from Video [107, Episode 06: 36:09]

Explain the ambiguities in the following sentences:

1. No-one likes Oxford and Cambridge students
2. Every nice girl loves a sailor
3. Our shoes are guaranteed to give you a fit
4. Irritating children should be banned
5. Why do swallows fly south for winter?

Answers from Video [107, Episode 06: 54:45]

3.7.6 Argument Analysis

1. Consider the following passage:

> The information revolution raises numerous ethical questions. We ourselves are now the resources – our bodies, our genes, our brains, even our attention, and our social world. This resource, 'human', will be exploited and depleted, both physically and mentally, in the same way that reckless farmers deplete fertile soil or a heartless capitalist exploits a labourer. A crucial question is therefore: what should be the leading principle in our efforts to avoid this scenario of exploitation?
>
> Two factors that could be a tentative key to the answer, however vague, could be: human dignity (for example, the right to respect, privacy, and physical and mental integrity) and human sustainability (the right to personal uniqueness: what aspects of humans and humanness are seen as manipulable, and what aspects would we like to keep?).

We are only concerned with the first paragraph. It is an argument. What sort of argument? What are the premises? What is the conclusion?

2. **Growing Trees**: The chanterelle, a type of wild mushroom, grows beneath host trees such as the Douglas fir tree, which provide it with necessary sugars. The underground filaments of chanterelles, which extract the sugars, in turn provide nutrients and water for their hosts. Because of this mutually beneficial relationship, harvesting the chanterelles growing beneath a Douglas fir seriously endangers the tree. Which of the following, if true, casts the most doubt on the conclusion drawn above? Why?

   A. The number of wild mushrooms harvested has increased in recent years.
   B. Chanterelles grow not only beneath Douglas firs but also beneath other host trees.
   C. Many types of wild mushrooms are found only in forests and cannot easily be grown elsewhere.
   D. The harvesting of wild mushrooms stimulates future growth of those mushrooms.
   E. Young Douglas fir seedlings die without the nutrients and water provided by chanterelle filaments.

3. **Employee Satisfaction**: In a study of factors affecting employee satisfaction, investigators polled staff at eight companies with over $100 million in revenues and benefits including flexible schedules and on-site daycare. The investigators found that overall satisfaction levels at the companies were high, that the companies enjoyed profit margins averaging over 20%; over the last five years, and that the rates of employee departures at these companies had varied between 1% and 5% over this period. Which of the following conclusions may be drawn from the information above?

   A. Flexible schedules and daycare are important benefits for raising overall levels of employee satisfaction.
   B. High profitability levels for companies with revenues over $100 million are most likely the result of high employee-satisfaction levels.
   C. Companies without daycare and flexible-schedule benefits have higher rates of employee departures than do those with these benefits.
   D. At least 95% of employees will stay for at least one year at some companies with daycare benefits.
   E. More companies have recently begun offering daycare and flexible-schedule benefits to attract potential employees who are also parents.

4. **Vehicle inspection program**: The new vehicle inspection programme is needed to protect the quality of the state's air, for us and for our children. Auto exhausts emission are a leading contributor to pollution and consequently ill-health. The government's long-term interests in the health of its citizens and in this area as a place to live, work, and conduct business depend on clean air. Analyse the argument and say what unstated assumption has been made by the author.

5. **Gambling Technology**: Gambling experts claim that with a sufficiently advanced computer technology any person with such technology will soon be able to win almost every time he or she bets on horse racing. Yet such a claim could never be evaluated, for losses would simply be blamed on immature technology. Which of the following, if true, would be most useful as a basis for arguing against the author's claim that the gambling experts' claims cannot be evaluated? Explain.

A. Some technicians using advanced computers have been able to gamble successfully more than half the time.
B. Gambling experts readily admit that it is not yet possible to produce the necessary computer equipment.
C. There is a direct correlation between the sophistication of computer technology available to a programmer and the gambling success he or she achieves with it.
D. Certain rare configurations of computer data can serve as a basis for precise gambling predictions.
E. Even without computer assistance, skilled gamblers can make a steady living from gambling.

6. **Consider the following premises**:

   a) All computer programmers who specialize in Visual C++ are internet savvy.

   b) None of the computer programmers in Charlie Corporation is internet savvy or specializes in Visual Basic.

   c) If Anne specializes in Visual C++ then Brian specializes in Visual Basic.

   If the statements above are all true, then which of the following must also be true?

   A. If Anne specializes in Visual C++, Brian is not internet-savvy.
   B. None of the computer programmers in Charlie Corporation specializes in Visual C++.
   C. If Anne is internet-savvy, she specializes in Visual C++.
   D. If Brian specializes in Visual Basic, Anne is not in the Charlie Corporation.
   E. Either Anne or Brian is internet-savvy

7. **Providing a Network of Supercomputers**: Why should the government, rather than industry or universities, provide the money to put a network of supercomputers in place? Because there is a range of problems that can be attacked only with the massive data-managing capacity of a supercomputer network. No business or university has the resources to purchase by itself enough machines for a whole network, and no business or university wants to invest in a part of a network if no mechanism exists for coordinating establishment of the network as a whole. Which one of the following best identifies a weakness in the argument?

   A. It does not furnish a way in which the dilemma concerning the establishment of the network can be resolved.
   B. It does not establish the impossibility of creating a supercomputer network as an international network.
   C. It fails to address the question of who would maintain the network if the government, rather than industry or universities, provides the money for establishing it.
   D. It takes for granted and without justification that it would enhance national preeminence in science for the government to provide the network.
   E. It overlooks the possibility that businesses or universities, or both, could cooperate to build the network.

   Please provide an explanation of your answer.

8. Consider the following argument: The growing popularity of computer-based activities was widely expected to result in a decline in television viewing, since it had been assumed that people lack sufficient free time to maintain current television-viewing levels while spending increasing amounts of free time on the computer. That assumption, however, is evidently false: in a recent mail survey concerning media use, a very large majority of respondents who report increasing time spent per week using computers report no charge in time spent watching television. Which of the following still has to be determined to provide a missing premise for the argument?

   A. Whether a large majority of the survey respondents reported watching television regularly
   B. Whether the amount of time spent watching television is declining among people who report that they rarely or never use computers
   C. Whether the type of television programs a person watches tends to change as the amount of time spent per week using computers increases
   D. Whether a large majority of the computer owners in the survey reported spending increasing amounts of time per week using computers
   E. Whether the survey respondents' reports of time spent using computers included time spent using computers at work

Chapter 4

Professional ethics

We have now seen the basic tools and concepts to consider ethical questions in ICT, a field we have chosen to call "computer ethics" (Section 3.1). We have considered a number of scenarios concerned with property rights, privacy, free speech, and development issues. Ethics in the profession has received cursory attention embedded in a scenario. For instance, the Volkswagen 'defeat device', on whether to do what your boss asks you to do. We will come across other scenarios in this chapter, which focuses specifically on the workplace, the roles of the people involved, and the sort of situations one may end up in that demands for an ethical analysis and judgement. If you are a first-year student reading this, it may seem too remote right now, but professional ethics also applies when you do an internship, sign up as a tutor, or are enterprising on the side with a few fellow students.

Because professional ethics is relevant for any job, one may ask oneself "are computer ethics different to those that came before?", or for other professions, for that matter. This is the first issue examined in this chapter (Section 4.1). Subsequently, several specific work-oriented scenarios will be presented, which introduce the various relevant aspects to consider professional ethics. We then tackle issues around computing as a profession in Sections 4.3, the typical types of relationships in the workplace (Section 4.4), and finally summarise codes of conduct relevant to IT (Section 4.5), all of which are intended to facilitate to better resolve the issues introduced in the scenarios. Finally, as integrative issue, we shall touch upon the thorny issue of accountability in Section 4.6.

4.1 Are Computer Ethical Issues Unique?

It should have become clear from Chapter 2 that ICT has had a profound impact on our society, especially since the 1980s, wherever in the world you are. Like in practically any area, it raises ethical issues every now and then. Opinions vary as to whether computer ethics are different, with the two common answers as follows [108, pp. 9–14]:

No, since all fields have similar problems and issues. There always have been issues of privacy, property, and freedom. The introduction of computers does not necessary introduce new ways of doing things. Often computers increase efficiency but fundamentally, the way of doing the task is still the same.

Yes, since a new technology has been introduced that never existed before and there are issues specific to computers such as the precise nature of programming, autonomous action, etc.

Tavani [108, p12] points out that we would commit a logical fallacy if we concluded that computer ethics issues must be unique simply because certain features or aspects of ICT are unique.

In the standard form (introduced in Section 3.6.1) this argument is:

ICT has some unique technological features.
ICT has generated some ethical concerns.
At least some ethical concerns generated by ICT must be unique ethical concerns.

This reasoning is fallacious because it assumes that characteristics that apply to a certain technology must also apply to ethical issues generated by that technology. So we cannot prove that the issues are unique but we must not rule that out either.

Moor [80] claims that computer ethics is not like any other; it is a new and unique area of ethics. The key differences in his view are:

- the truly revolutionary aspect of computers is their *logical malleability* — the first *universal enabling* technology,
- the computer's transformative impact on society, for example, as robots do more and more factory work, the emerging question will not be merely "How well do computers help us work?" but "What is the nature of this work?" and
- the invisibility factor — most of the time computer's actual operations are invisible. A problematic example of invisible abuse is the use of computers for surveillance. Another is the invisibility of the calculations: "Computers are used by the military in making decisions about launching nuclear weapons. On the one hand, computers are fallible and there may not be time to confirm their assessment of the situation. On the other hand, making decisions about launching nuclear weapons without using computers may be even more fallible and more dangerous. What should be our policy about trusting invisible calculations?"

Johnson [59] argues that "computers and ethics are connected insofar as computers make it possible for humans to do things they couldn't do before and to do things they could do before but in new ways. These changes often have moral significance." She makes the claim that, far from computer ethics being part of "normal" ethics we may well reach a stage where, as we become more and more accustomed to acting with and through computer technology, the difference between "ethics" and "computer ethics" may well disappear.

Donald Gotterbarn [45][108, p. 16], on the other hand, is not convinced by an argument about ICT being a new technology. For example, he argues that there was no new ethics

called "printing press ethics"[1]. As for malleability or flexibility he sees that as due to the underlying logic — and we did not develop logic ethics.

The newness leads people to think that computer ethics has not yet found its primary ethical standard and so we cannot make ethical decisions.

Gotterbarn regards claims of ethical uniqueness as dangerous. It leads one to think that not only are the ethical standards undiscovered, but the model of ethical reasoning itself is yet to be discovered. "We have mistakenly understood computer ethics as different from other professional ethics", he states. The distinguishing characteristics among professional ethics, is the context in which they are applied, not distinct sets of ethical rules or different kinds of moral reasoning.

4.1.1 A Three-step Strategy for Approaching Computer Ethics Issues

We saw in Section 3.2 that computer ethics is applied ethics. So how do we apply it? We need to make computer ethics relevant to the typical computer professional: A professional has technical skills but also makes ethical decisions. While there may be policy vacuums, the ethics for computing professionals is not another kind of ethics: it is ethical values, rules and judgements applied in a computing context based on professional standards and a concern for the user of the computing artefact.

Before we can start with the case analyses, we need to establish the context and stakeholders as outlined in Section 1.2. Tavani then outlines a *three-step strategy for approaching computer ethics issues* [108, pp. 27–28] as a *guide* rather than a definitive algorithm of some kind:

Step 1. *Identify* a practice involving information and communications technology, or a feature of that technology, that is controversial from a moral perspective.

- **1a.** Disclose any hidden (or opaque) features or issues that have moral implications
- **1b.** If the ethical issue is descriptive, assess the sociological implications for relevant social institutions and socio-demographic and populations.
- **1c.** If the ethical issue is also normative, determine whether there are any specific guidelines, that is, professional codes that can help you resolve the issue.
- **1d.** If the normative ethical issue cannot be resolved in this way then go to Step 2.

Step 2. *Analyse* the ethical issue by clarifying concepts and situating it in a context.

- **2a.** If a policy vacuum exists, go to Step 2b; otherwise, go to Step 3.
- **2b.** Clear up any conceptual muddles involving the policy vacuum and go to Step 3.

Step 3. *Deliberate* on the ethical issue. The deliberation process requires two stages.

- **3a.** Apply one or more ethical theories (see Section 3.2) to the analysis of the moral issue, and then go to Step 3b.

[1] Although one might consider the ethics of censorship and copyright as originally being necessitated by the invention of the printing press.

3b. Justify the position you reached by evaluating it via the standards and criteria for successful logic argumentation (Section 3.6).

4.2 Scenarios

Now let's try to apply the three-step strategy to the following scenarios.

Scenario 1: How much Security?

Thembi has a computer science degree and three years of work experience. She has her own company. One of the current projects involves designing an employee database for a large company. The database contains medical records, performance evaluation, salary etc. She must decide on the security required for this system. The question is: how much security?

She believes that the client should have all the necessary information that the client can use to base their decision on. She then presents *all* available options to the clients, with the level of security proportional to the cost. The client chooses the cheapest and least secure option, which leads Thembi to feel that this is insecure. She explains the risks to the client, but they stick with the cheapest option.

- Should Thembi refuse to build the system?
- Was it right to present this option to the client in the first place?

Scenario 2: Conflict of Interest

Juan is a private consultant. His job is to evaluate automation needs and recommend suitable systems. Recently he was hired by a hospital to upgrade their systems. He recommended (with reasons) Tri-Star as a best system to upgrade to. However, he failed to mention that he is a partner in Tri-Star and that there is a conflict of interest. Was his behaviour unethical? Should he have:

- Declined the job originally
- Disclosed his ties with Tri-star?

Scenario 3: Safety Concerns

Carl works for general purpose software and hardware company on a project for the Department of Defence (DoD). The project involves developing a system that monitors radar signals for missiles and launches nuclear missiles when deemed necessary. Carl was initially reluctant but eventually agrees. His thinking was that if he does not do it, someone else will anyway. During his work he develops some reservations concerning the fine distinction

between missiles and small planes. He expresses this to his manager who promptly dismisses the claim on the basis that he does not agree with the claim and that the project was already late. Carl feels morally responsible. What should he do? What can he do?

- Ask for re-assignment;
- Go higher up in his company with his worries;
- Go to the contractor, in this case the DoD;
- Go to newspapers (blow the whistle) — this will likely lead to him losing his job.

4.2.1 What does it mean to act as a Professional?

The three scenarios illustrate difficult situations. To solve them we could use utilitarian or deontological theories, among others, but they are only useful if the contexts of the problem are taken into account:

- Carl is a professional and employee;
- Thembi is a professional, owner of the company and has a contract with a client.

In these situations, we must consider what it means to act as a professional. What responsibilities do:

- Employees have to employers and vice versa;
- Professionals have to a client and vice versa;
- Professionals have to the public.

Exercises

Reflect on the previous examples, write down an initial answer, and then revisit them once you have completed this chapter. You may want to consider the following questions in your answer:

- If we say the people involved were (or should have been) professional, what do we mean?
- In what way are they distinguished from their clients, employers, the rest of the public?
- Who are they answerable to?
- How can one know, objectively, that someone is a professional?
- What should guide the actions of professionals?

4.3 Characteristics of a Profession

We must recognise that a professional role is special because it carries special rights and responsibilities. Some occupational roles are said to be *Strongly Differentiated* where by professionals are granted powers exceptional to ordinary morality (e.g., consider medical doctors). Most occupational roles are *not* strongly differentiated. It is claimed by most that the computing profession is *not* strongly differentiated, i.e., computer professionals do not acquire special power/privilege by virtue of being in the profession. However this is not always the case — when hired to do a job, professionals do acquire powers and hence obligations that come with them. For example, Carl has an obligation to his company but also to society: he does not have to do everything his boss asks. Thembi has obligations to the client for the security that they want.

A *profession* is an occupation one follows in which one professes to be skilled in.

Any profession involves a mastery of *expert knowledge* (or esoteric body of knowledge). This is usually possible for each individual by acquiring by a higher education degree. Disciplines generally embrace a division between researchers and practitioners.

Members of a profession are *autonomous* in their work. They make decisions and do not take orders from others, with the exception of work assigned to them by their employers or clients. They need to be able to regulate themselves and set their own admission standards. Moreover, disciplines also have standards of practice.

This is possible because there is often one unifying *formal organisation* which is recognised by the State. The responsibility of such an organisation is to control admissions to the profession, it accredits educational institutions, sets up and administrates disciplinary procedures, and has the power to expel members.

It also has a *code of ethics* that sets standards of itself in order to maintain its autonomy. Members must adhere to its code irrespective of their employment contexts.

Furthermore, a professional must been seen to fulfil some useful and important *social function*.

There are three types of computer professional certification for individuals. In particular, we have vendor-specific, vendor-neutral, and general certification. The first two are used by companies and third parties to certify individuals to prove that they are proficient in servicing certain products. The third one is of particular interest. They are used to admit one to a regional or international body of professionals, who do not necessarily service a specific product. These are individuals who are required to abide by a body's policies.

4.3.1 System of Professions

Many groups wish to be considered professional. They wish: 1. Self regulation; 2. Status; 3. High salaries. They need a monopoly to achieve this. To achieve this status the group needs to be organised into a formal grouping. They must also demonstrate a domain of activity and that if the group has control over this domain that it will be safer and more effectively run. The group must convince the public that lay people can not adequately judge

the group and that only the group themselves are capable of judging themselves. Usually professional monopolies are granted on conditions that they must regulate themselves and that they must further the interests of the public.

This means that a professional group must:

- Convince the public of their special knowledge;
- Show that important social functions are at stake;
- Convince the public to trust the group (usually by means of code of Ethics)

For success the group needs a formal organisation to give the group a monopoly. Collective autonomy for the group justifies individual autonomy for members. The Information Technology profession is self-regulated. This is unlike statutory bodies such as Health Professions Council (HPCSA) and Engineering Council of South Africa (ECSA).

4.3.2 Is Computing a Profession?

The computing field is young and very broad. This is in sharp contrast to the medical and accounting fields. It is also very malleable and it is used in many domains, such as teaching, engineering, libraries etc. Some of these workers are not seen as computer professionals. So is computing a profession?

We compare computing with the five characteristics of profession.

Mastery of Expert Knowledge: Many do acquire knowledge through higher educational institutions. This is more true as time goes on. There also exists a division between researchers and practitioners. There is a large demand as many in the field have inadequate knowledge.

Autonomy: This is not strongly differentiated, i.e., there are no jobs that only professionals can do that others can not.

Formal organization: There are many such organizations in many countries such as IITPSA (Institute of Information Technology Professionals South Africa) and the BCS (The Chartered Institute for IT — was British Computing Society).

Code of conduct: There is no single code worldwide but several do exist. BCS has a comprehensive code[2], and IITPSA also has a code of conduct[3].

Fulfilment of a social function: Computing is a crucial part of society, and it does fulfil a need. It supports a variety of social functions but is not one in itself, in other words it is a *(universal) enabling technology*.

Software engineering (development of a software system) might seem like a good area of computing for professionalism. Its activities involved unique knowledge, education, licensing of members and code of ethics.

[2] `http://www.bcs.org/category/6030`

[3] `https://www.iitpsa.org.za/codes-of-conduct/` and `https://www.iitpsa.org.za/codes-of-behaviour/`

4.4 Professional Relationships

Computer professionals may find themselves in a number of relationships within a society. In particular, they can participate in employer–employee, client–professional, society–professional and professional–professional relationships.

4.4.1 Employer – Employee Relationships

The first relationship involves a number of conditions, and these are often explicit in the contracts (e.g., responsibilities and salary) but many important issues are left out or unclear (e.g., overtime). There are also some conditions which are specified by a country's laws such as sick and annual leaves, while some are negotiated by unions (e.g., retrenchment rules). The moral foundation for this relationship is contractual. Individuals should be treated with respect and not merely as a means. Neither party should take advantage of the other. All things being equal, an employee should be loyal to his or her employer and *vice versa*.

The employee should be honest with their experience and qualifications. The employer should not exploit the employee (they should provide a decent wage, safe and healthy working environment, etc.). In working for an employer, an employee may acquire trade secrets or specific knowledge in a field. Such information may be governed by a non-disclosure agreement such as a contract not to reveal these or not to work in this area for period. In general, it is unethical to sell specific knowledge but generic knowledge and experience gained in a field helps employees get a better job. It is fine to use generic knowledge to progress in one's career.

Example 4.1: Employer-Employee relationships issues: Uber and Waymo.

> A dispute of this transfer-of-knowledge, or inside-information claims, arose recently between Uber and Waymo, the self-driving car unit of Alphabet (Google). At the heart of the issue is Anthony Levandowski a former engineer in Google's autonomous vehicles division. When he left Google, Mr Levandowski started his own firm, Otto, which Uber then bought six months later. Waymo alleged that Uber stole trade secrets from it. A key piece of evidence is that Mr Levandowski downloaded 14,000 documents from Waymo shortly before leaving[a].
>
> [a] `https://www.ft.com/content/fe2bb4e8-6a38-3039-abdc-049096bece84` and `https://www.nytimes.com/2017/05/30/technology/uber-anthony-levandowski.html`

4.4.2 Client – Professional Relationships

Recall Scenario 3 above, where Carl expressed concerns about safety. His company should have told the DoD that the project was late. In this respect, his company was not acting

well. Additionally Carl tried to work through his company but failed. The client (the DoD) depends on professional for the knowledge and expertise in the special area.

There are different models for this kind of relationships:

Agency: The professional is the agent and does exactly what the client tells him to do (like telling a stockbroker to buy "Telkom").

Paternalistic: The professional makes all the decisions and the client abrogates all decision making.

Fiduciary: Both parties play a role by working together. The professional offers options while the client decides which one to take. This requires trust on both sides and that the decision process is shared

> **Fiduciary**
>
> *Fiduciary* = based on trust. A fiduciary is a person who holds a legal or ethical relationship of trust with one or more other parties (person or group of persons). This requires the professional to provide the client with options for major decisions. Such a process requires trust from both sides, and decision making is shared.

Recall Scenario 2 above (Section 4.2) where Juan recommended a company in which he had an interest. This is in breach of the relationship with his client. It is wrong to withhold this information and could be self-serving, although if he were to exclude the company in which he has an interest he may give client poor advice.

4.4.3 Society – Professional Relationship

This relationship is usually shaped by law, but the law (or people who make them) can not foresee everything, especially in a rapidly moving field such as IT. If society licenses a professional society then the professional society must serve the interests of Society in general and must take due care based on the special knowledge it possesses.

Special Obligations to Society

Some computer corporations may have some special moral obligations to society because of their profound societal impact. For example:

Search engine companies have a crucial role in the access to information. Issues include: 1. Search engine bias and nontransparency; 2. Privacy, consent, and non-voluntary disclosure of personal information; 3. Monitoring and surveillance; 4. Democracy, censorship, and the threat to liberty and freedom.

Developers of autonomous systems and robots are held responsible for "moral-decision-making software code" built into them.

There may be conflicting responsibilities towards an employer and towards society. Consider Carl's case again—the company needs contracts to survive but Carl's concern is his responsibilities to society. So when does a professional 'rock the boat' when it comes to society versus other relationships? There is no easy answer, but, generally:

- Professionals must be convinced of their position;
- Professionals must consult managers at different levels first;
- If they become whistle-blowers, they might lose their job.

Whistle-Blowing

Whistle-Blowing refers to revelations meant to call attention to negligence, abuses, or dangers that threaten the public interest.

"Whistle-Blowing is central to ... constitutional principles. It is key in the fight against corruption and mismanagement, especially of public funds, and to strengthening transparency and accountability within organisations and society more generally." Adv K Malunga Deputy Public Protector South Africa, 28 January 2015 [73].

In South Africa there is a concept of *Wider Disclosure* or *General Protected Disclosure*: whereby an individual may disclose sensitive information to the police, MPs or the media. This only applies if the whistle blower honestly and reasonably believes that the information and any allegations contained within are substantially true, and that the disclosure is not made for personal gain. The South African law recognises four justifiable causes: 1. The concern was raised internally but was not addressed properly; 2. The concern was not raised internally because he/she believes he/she would be victimized; 3. The concern was not raised internally because he/she genuinely believed a cover-up was likely; 4. The concern was/is exceptionally **serious**.

NB: Standard disclaimer: This is not legal advice! Consult a lawyer or union if this situation arises for you[a].

[a] See for example `http://www.labourguide.co.za/discipline-dismissal/667-the-protection-of-whistle-blowers` or `http://www.opendemocracy.org.za/`

Whistle-blowing can be viewed as being slightly different from anonymous leaks. The main difference is that the identity of the individual who exposes the information is known and it is based on a conviction that their actions serve the public. Whistle-blowers are generally not viewed in a positive light by their institutions.

Society and public policy

A community is a group of people who share social, economic, or political interests. Groups of this nature also tend to share common 'universal' values. A value need not be accompanied or enforced by a law. There are individuals who view the law as simply a collection

Example 4.2: Edward Snowden: Whistle-blowing about mass surveillance.

> An example of a whistle-blower is Edward Snowden, an US citizen who worked for the United States of America's (USA) Central Intelligence Agency (CIA), and a US (United States) government defence contractor. He is well-known for sharing confidential National Security Agency (NSA) documents with the purpose of exposing the USA government's mass surveillance program. His whistle-blowing resulted in him fleeing the USA and being granted temporary asylum in Russia. He was subsequently charged for his actions by the US' Justice Department with theft and two counts of the contravening the US's 1917 Espionage Act [37]. After revealing the information to journalists, he willingly unmasked himself to the public because he had "no intention of hiding [himself] because [he knew that he had] done nothing wrong" [47]. Here, we see an individual whose values went against that of his employer, who is sure of his position, and is prepared for the consequences of his actions. Moreover, his actions are in the interest of the public good.

of norms which are mandatory to all members of the society. Moreover, these norms are related to the values held by a society [33]. This relationship need not be affirmative. In particular, there are cases in which laws and values conflict: one simply has to consider the South African apartheid legislation to see this.

An important aspect of a democracy is public participation in crafting public policy. In practice, it is difficult for regular members of the public to participate in these processes in a meaningful way due to overwhelming information (truth and misinformation) directed at them. Furthermore, the language used in these processes is often not suitable for individuals without expert knowledge [127]. Computing professionals are members of the public who have the capability to grasp the language used. A decrease of computing professional participation in the crafting of public policy diminishes the number of parties who are able to engage the government on issues of science and technology. This has the potential to lead to a disengaged citizenry thus leading government to only consult professional bodies. This has the potential of the public not being able to engage lawmakers about potential risks which may be ignored or concealed by professional bodies [92]. Computing professionals agree to a code of ethics which binds them to an obligation of improving the lives of those who use computers. In particular, it is the responsibility of the computing profession to improve the understanding of the public about issues pertaining to computer systems [71]. A professional need not directly contribute in the drafting of legislation. They can contribute in the education of the public about specific policies.

4.4.4 Professional – Professional Relationships

Many believe that this relationship is self-serving. They see members as only having an obligation to other members. This might create a reluctance to criticise another professional. Often such scenarios are complex, especially when it is difficult to tell whether it's a genuine

error or incompetence. For a professional society to flourish there must also be advantages to Society from it: 1. Members to consider what they owe to each other to maintain standards of conduct; 2. There is a need for disciplinary hearing procedure.

4.5 Professional bodies' codes of conduct and practice

A code of ethics is a statement of collective wisdom of the members of the profession that expresses experience and consensus of many members. Its function is to serve and protect the interests of the public and promote worthy practices. It is a statement of shared commitment of members of the profession, agreed values and rules. It sensitises members to important issues, and is a mechanism for educating those entering the profession, companies, and clients. The code also ensures collective responsibility, so that various parties do not only think of individuals in the profession but rather a collective unit of the profession. If a profession speaks out on an issue, it is more effective as a group. Examples of this are issues such as protection of whistle blowers and gender bias. There are professional bodies which are responsible for professional certification.

Common themes for ethical behaviour for computer professionals:

1. Personal integrity / claim of competence;
2. Personal responsibility for work;
3. Responsibility to employer / client;
4. Responsibility to profession;
5. Confidentiality of information / privacy;
6. Conflict of interest;
7. Dignity / worth of people;
8. Public safety, health, and welfare — serving the interests of the Public;
9. Participation in education / professional societies.

Apart from the IITPSA (see Section 4.5.1) and BCS (see Section 4.5.2), other computer professional bodies with similar responsibilities are the Association for Computing Machinery (ACM), the Association of Information Technology Professionals (AITP), the Systems Administrators Special Interest Group of USENEX and more [71]. Their documents are incomplete by design as it is not possible to compile a document that will list all the possible actions to take in all circumstances. It is for this reason that policy document are written in a general language [71]. In the event that the policies of the workplace are not able to prescribe the appropriate action to take in a certain circumstance, professionals should rely on the policies of professional bodies.

4.5.1 Code of Conduct: Institute of Information Technology Professionals South Africa

The IITPSA Code of Conduct[4] is summarized as follows [56]:

- Act at all times with integrity;
- Act with complete loyalty towards a client when entrusted with confidential information;
- Act with impartiality when purporting to give independent advice and must disclose any relevant interests;
- Accept full responsibility for any work undertaken and will construct and deliver that which has been agreed upon;
- Not engage in discriminatory practices in professional activities on any basis whatsoever;
- Not seek personal advantage to the detriment of the Institute, and will actively seek to enhance the image of the Institute.

The Institute is ready at all times to give guidance in the application of the Code of Conduct. In cases where resolution of difficulties is not possible informally, the Institute will invoke the disciplinary procedures defined in its Memorandum of Incorporation and associated Rules.

IITPSA Code of Practice is directed to all professional members of the Institute. The Code is concerned with professional responsibility. All members have responsibilities – to clients, to users, to the State and to society at large. Those members who are employees also have responsibilities to their employers and employers' customers and, often, to a Trade Union. Since IITPSA membership covers all occupations relevant to the use of Information and Communications Technology and it is not possible to define the Code in terms directly relevant to each individual member.

4.5.2 BCS Code of Conduct

The BCS, for example, sets the professional standards of competence, conduct, and ethical practice for computing in the United Kingdom. It should be noted that its members need not be UK citizens. The body has a code of conduct of which all its members need to abide. These rules of the conduct can be grouped into the principal duties: the public interest, professional competence and integrity, duty to relevant authority, and duty to the profession.

The BCS code deserves special mention since the IITPSA code was originally inspired by it. The UCT Department of Computer Science is accredited by BCS in the absence of such a body in South Africa.

[4] `https://www.iitpsa.org.za/codes-of-conduct/` & `https://www.iitpsa.org.za/codes-of-behaviour/`

Like the IITPSA, the BCS has retired the existing Codes of Good Practice as these did not provide comprehensive coverage. Such codes are not sustainable in a field as diverse as IT where there is such rapid change. It is copied here:

The Public Interest

You shall:

a. have due regard for public health, privacy, security and wellbeing of others and the environment;
b. have due regard for the legitimate rights of Third Parties;
c. conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement;
d. promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise.

Professional Competence and Integrity

You shall:

a. only undertake to do work or provide a service that is within your professional competence;
b. **not** claim any level of competence that you do not possess;
c. develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field;
d. ensure that you have the knowledge and understanding of Legislation and that you comply with such Legislation, in carrying out your professional responsibilities;
e. respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work;
f. avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction;
g. reject and will not make any offer of bribery or unethical inducement.

Duty to Relevant Authority

You shall:

a. carry out your professional responsibilities with due care and diligence in accordance with the Relevant Authority's requirements whilst exercising your professional judgement at all times;
b. seek to avoid any situation that may give rise to a conflict of interest between you and your Relevant Authority;
c. accept professional responsibility for your work and for the work of colleagues who are defined in a given context as working under your supervision;

d. **not** disclose or authorise to be disclosed, or use for personal gain or to benefit a third party, confidential information except with the permission of your Relevant Authority, or as required by Legislation;
e. **not** misrepresent or withhold information on the performance of products, systems or services (unless lawfully bound by a duty of confidentiality not to disclose such information), or take advantage of the lack of relevant knowledge or inexperience of others.

Duty to the Profession

You shall:

a. accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute;
b. seek to improve professional standards through participation in their development, use and enforcement;
c. uphold the reputation and good standing of BCS, the Chartered Institute for IT;
d. act with integrity and respect in your professional relationships with all members of BCS and with members of other professions with whom you work in a professional capacity;
e. notify BCS if convicted of a criminal offence or upon becoming bankrupt or disqualified as a Company Director and in each case give details of the relevant jurisdiction;
f. encourage and support fellow members in their professional development.

4.5.3 Strengths and Weaknesses of Professional Codes

Professional codes aim to assist in revenging and resolving ethical issues, but, given the many debated cases, they are not 100% effective. However, this does also not mean one should throw out the baby with the bathwater. Here we list their main strengths and weaknesses on how it works our in praxis.

Strengths	Weaknesses
inspire the members of a profession to behave ethically.	Directives included in many codes tend to be too general and too vague
guide the members of a profession in ethical choices.	Codes are not always helpful when two or more directives conflict.
educate the members of a profession about their professional obligations.	A professional code's directives are never complete or exhaustive.
discipline members when they violate one or more of the code's directives.	Codes are ineffective (have no "teeth") in disciplinary matters.
"sensitise" members of a profession to ethical issues and alert them to ethical aspects they otherwise might overlook.	Directives in codes are sometimes inconsistent with one another.
inform the public about the nature and roles of the profession.	Codes do not help us distinguish between micro-ethics issues and macro-ethics issues.
enhance the profession in the eyes of the public.	Codes can be self-serving for the profession.

4.6 Accountability in IT

Now that we have seen roles in the workplace and codes of conduct on how to behave in general, we should be able to answer the previously introduced case studies. However, there is a snag that we haven't considered yet: who can be held accountable? This can go in either way: *who's responsible when things went wrong?* and *who is responsible when things went well?* Such a responsibility is directly linked to the concept of *moral agency*: if one has it, one may be held responsible.

This is easier said than determined in practice, however. To highlight some issues and start disentangling this, we shall first describes a few scenario.

Moral agency

Moral agency applies when the following conditions are met:

i) whether the ethically relevant result is an outcome of the agent's actions (i.e., causality);

i) whether the agent had or should have had knowledge of the consequences of its actions; and

i) whether the agent could choose another option (generally considered as to be without greater harm for the agent).

Conversely, when at least one of the three conditions is absent, one is, generally, not held morally responsible for the act.

4.6.1 Scenarios

Scenario 1: Designing-making Systems

David works for an investment company. His job is to pick investments for a pension fund. To help him make decisions, he uses an expert system. Each upgrade of the system gives more complex analysis. David is very nervous about the market this week. His personal indicators point to the market going down, while the expert system points to it going up. The system recommends that he puts substantial investments into the market but he does not understand the system's analysis. He also can not judge if the system is defective.

What do you think David should do? Should he go with his own analysis and feeling or go with the expert system? Note that if he makes the wrong choice, he will lose a lot of money for his company. Also consider the following questions:

- Can David be held responsible if he uses the information of the program and that turns out to be the wrong decision?
- Can the system's designer or owner be sued or held responsible if the system is working properly? What about if the system is found to be faulty, should the designer pay back the money lost by the investment company?

Scenario 2: Service Provider for Online Forums

Milo is a freelance journalist and specialises in Southern African politics. She uses the Internet to keep up to date and uses her computer to write articles, news, as well as taking part in online chat rooms and forums. She has been away and on her return, she is outraged to find postings on a forum attacking her. In these postings, it was claimed that she is a drug dealer and that her stories are filled with lies. In response, she posts a denial and also contacts the forum administrator for names and address of the defamer (All posters are required to register with their real names and address for billing purposes). However, the forum administrator refuses to give her this information. Milo is now suing them because she can not sue the perpetrator.

- Do you think the forum administrator should be responsible for what is said in the forum?
- Can the company providing the software be held responsible?
- If neither, then who should be? If both, in what proportion?

Scenario 3: Y2K Problem

The infamous Y2K problem was a result of saving precious memory space by truncating year information to two digits (e.g., 1975 is stored as 75). As the year 2000 approached, calendar dependent activities were at risk. Some software clearly would be affected, but for others, the code was quite impenetrable and no-one knew if it did anything with dates. The public reacted to this with disbelief and outrage. Were the professionals asleep? Was it a ploy

for companies to employ more professionals and charge their customers to fix this issue? Should the manufacturers and designers have had more foresight? Why was more not done earlier to address the issue? Who should pay for the costs to check and fix the software?

The year 2000 arrived with no major catastrophe and, in fact, there were only a few isolated problems. Various opinions have been expressed on this issue. Some saying that the problems were fixed on time; while others saying that the problem was overstated.

- Can the person who came up with that original idea of truncating the year to just two digits instead of four be held responsible?
- Should all the software engineers who coded the year into two digits be held responsible (if it can be identified who wrote those particular lines of code)?
- Could the coders blame their managers, who were promising clients fancy features such that they were compelled to truncate the year in order to meet the design specs?
- Who else may be responsible?
- Is this even a case of *blame* and maybe it was reasonable to assume that code written in, say, 1980 would not still be in production by 2000? That is, it is, at most, a mistake in judgement, but surely not a bug?

4.6.2 Ensuring Accountability

Computer systems are powerful and can cause harm financially, physically, or psychologically. To be mindful of this, is one of the professional duties identified in most codes of ethics and/or conduct. One approach would be to find appropriate laws and to use them. However, different laws apply in different situations; for example, one law might be applicable to defective product, while others to negligence.

Another factor is the rate of change of the technology. Typically it can take a long time to pass a piece of legislation, by which time the technology might have evolved. This relates to the *policy vacuum* that passed the revue in Section 3.4.1. In addition to relying on legislation, we can also employ a mixed approach in terms of accountability, responsibility, liability and blame. We will discuss these terms individually:

Accountability This is used in its broadest meaning. It refers to the appropriate agent to response and depends on various factors. For example, in a department in a company, the head of department might be held accountable. Accountability rests with someone with the ultimate responsibility.

Responsibility There are many types of responsibility:

Role Responsibility This is analogous to duty. It is what people are expected to do within their role.

Casual Responsibility This is a responsibility as a result of causality. For example, X did something and caused an event to happen. David invests a large amount of money in the Market and causes the company to lose money, even though David might have done all that was required of his duty.

Blameworthy Responsibility David may or may not be responsible, but he is not blameworthy. Perhaps the software was faulty? In that case, the software designer might be blameworthy if he failed to fulfil a role responsibility.

Liability A friend slips on the polished floor of your house and break a leg. You might be held liable but you may not be blameworthy.

Buying and Selling Software

First of all: is buying or selling software any different from buying and selling anything else? Let us look at the various responsibilities of the buyer and seller. The *seller* has the right to sell, a duty to be honest, a duty not to coerce a client, is expected to emphasise the good aspects of the product and to answer questions honestly. Is a seller being dishonest if they do not disclose a problem area not asked about? This is probably the case, but it is very difficult to say, especially if the user's needs are varied and complex and may not even have to right vocabulary for it and it may be hard to establish by the seller what the needs of the buyer are. Usually, the product itself (either packaging or licence agreement) will contain all the necessary information. A contract can be voided if all relevant information is not given. The *buyer* has the responsibility to find out all the necessary information and ask the right questions.

The question then is: is *software* like any other item? This is not fully clear. For instance: is it a product or a service? This depends on the circumstances of how the software is produced and/or sold. A comparison can be made between software and buying a suit[5], for which there are three types:

- Off the peg / Ready to wear (no alteration)
- Tailor made to specific requirements of person
- In between (off the peg + alterations)

For software a similar groupings can be made:

- Mass market (a product)
- Customised software (service)
- Mixed (Product + service)

Yet, just that it is tailor made, does not mean 'software' becomes another kind of thing—software is software (whatever it is ontologically)[6]. The concept of *software as a service*, or SaaS, does exist, however, which is a key concept within the area of distributed computing (including cloud computing). SaaS delivers applications to customers on a sort of rental agreement and is run from a central organisation, such as Amazon Web Services, using Googledocs from Alphabet Inc, or booking a slice of the HPC Cluster from ICTS@UCT.

Further, depending on whether software is a service or a product, different laws will apply. For instance, when you buy a product, you own the product and can do with it what you

[5] An earlier version of the notes attributed this list and analogy to "(Prince 1980)", but the reference is elusive.
[6] Recalling the previous chapter on reasoning by analogy: is this analogy a good one? If not: why not?

want; yet, one can pay for a service, but then you still do not own the service provided. To complicate matters: laws in different countries are likely not exactly the same on services, so—if there's no policy vacuum—then likely neither on SaaS regulations. But what if you use the SaaS in, say, South Africa, but it's run from a server located in the United States? Whose laws should apply?

Mass Market Products With mass market, strict liability can be imposed on this type of product. Producers can be sued for errors or malfunctions causing damage because: i) Producer puts the product in the public domain and invites people to buy or use it, ii) Producer earns profit and should bear the risks, iii) Producer is in the best position to anticipate and control the risks associated with the product, thus the onus is on the producer to get the product right; iv) Producer can spread the cost of injury and insurance over all clients.

Customised Software Strict liability does not make sense here as software is created and designed specifically for a client. The client knows the context in which the software will be used and so specifies what is required. The client thus needs to take part of the risk. This type of software should thus be considered as a service.

Mixed Case The product and service should be treated each on its own.

Negligence

Negligence is a failure to do something that is expected of a reasonable and prudent person. For example, if a security guard is knocked unconscious, he cannot be blamed, but if he is drunk, he might be considered negligent. There is always presumption of a reasonable standard of behaviour. Often this is used to describe blameworthy behaviour of professionals.

The definition of a standard applicable to the offence is often quite difficult to arrive at. Often this is best judged by other professionals, assuming they behave professionally and are not influenced by a conflict of interest.

Example: Y2K Problem

In the end, companies involved did a lot of checking and spent a lot of money in correcting the problem—resulting in no serious disasters. However, the question of responsibility remains. Who should pay for the cost of upgrading or modifying relevant hardware or software? For instance: Hardware Manufacturer, Company using the computers, Computer Professionals who designed the system, Professional Society, all of the them?

Who was responsible? Consider the following timeline.

1970: 2 byte data for storing year information saved expensive space – the professionals did a good job.

1980: Same answer

1990: Same answer? Were the systems expected to last for 10 years? What is the cost of storage at this time? What is the cost of upgrading old system?

1995: Same answer? Were the systems expected to last for 5 years? Storage and upgrade cost? Should professionals warn companies of the Y2K problems? Should the IITPSA have a recommended code of Practice concerning this issue?

1998: Same question, different answer? Client companies all had policies. These were communicated to the shareholders and everyone accepted their responsibilities.

So it has been a lesson. The best strategy is:

- State clearly the role responsibilities of all concerned. Professionals needed to explain and document the problem and then to offer options.
- Make sure that all involved understood the effect of their work on humans. Clients needed to understand available options – they needed to realise that the option of staying with 2 digits was short-term and unsafe.
- Hold those responsible who fail to live up to their responsibility.

Diffusion of Responsibility

In creating a computer system appreciate the following:

- Scale and complexity of the system
- The number of people involved in development, distribution, training and using it.
- What the system will be involved in – many will be involved in important decision making.
- Kant: Humans are responsible for their actions because they have the capacity to control their action.

On the whole, though, this diffusion of responsibility makes it practically difficult in many cases to assign blame and responsibility, especially regarding some sort of 'amount' of responsibility, and blame and possible punishment when things go wrong. this is also called the *problem of the many hands*. For the Y2K problem, very many people in multiple organisations were involved in a range of decisions that ultimately led to the issue. For Volkswagen's "defeat device", also multiple people may be assigned various amounts of blame, though ultimately, generally, the bucket stops with a company's CEO. Two 'classical' examples are described next.

Example: THERAC-25 THERAC-25 is a computer-controlled system that gives radiation treatments to patients. Several patients received massive doses, resulting in at least three fatalities. It was difficult to discover who was responsible, but Therac was liable and paid compensation to the victims families. Eventually it was found that the action of the operator has caused the accidents. However, it was also found that if an operator entered incorrect mode, noticed this and corrected the error (within 8 seconds as specified), the system still went wrong and the patient was killed as a result. Thus while the operator caused the accident they were not to blame.

The error was traced to also exist in previous version of the software, but had caused no problems because there was only one mode in that version. Was it the designer or the tester (who looks for errors and unconformities to the requirements) who was at fault? The Therac case also illustrates the difficulty of testing real-time systems. Should there have been a feature on the system limiting the radiation dose to some MAXIMUM irrespective of everything else. If so, should this not have been specified by the clients? Are they also partially to blame?

Example: ISP Responsibility Recall the scenario with Milo, a service provider provides him with chat rooms and forums facilities. Milo was defamed by another user and has the right of recourse. The obvious route to deal with this is to hold the 6 individuals responsible – the problem is that the individual is anonymous.

Stratton versus ISP Prodigy (1995). Prodigy was sued by users with respect to content in its online forums which Prodigy has advertised that it has editorial control over. The court has applied the law governing newspapers and found Prodigy guilty. However, Prodigy claimed that they were like a telephone company and not newspaper company. The following year, the US Communications Decency Act reversed this on the basis that ISPs are closer to telephone companies. The act also introduced the Good Samaritan immunity in which an entity can exercise control without liability and is encouraged to do so.

Chapter 5

Intellectual Property

The issue of intellectual property rights has become one of the defining ethical issues of the digital era [108, p230], and the last word has not been said about it yet. Besides regulatory issues, grey areas, and gaps, one could argue it is one of the areas used by big companies in developed countries to disadvantage new entrants to the information society.

In this (too brief) chapter[1], we summarise the main IP protection mechanisms that are available and used (Section 5.1) as well as alternatives to these regimes that aim to foster open source, content, and standards (Section 5.3), interspersed with a few scenarios (Section 5.2).

5.1 Intellectual Property Protection

We could argue that an intellectual property (IP) right is a type of "natural right" that should be granted to individuals for the products that result from their labour. A more utilitarian approach is that IP is designed to promote progress, this is the view that is generally and historically favoured. Thus, there is a fair exchange for mutual benefit:

- Creator gets limited exclusive rights
- Society gets disclosure of inventions and creative works,

Thus an incentive is created for inventors and authors to create and disclose their work.

The types of intellectual property and their length of protection granted are:

Design Does not cover how the article functions (unlike patent) Protects the physical appearance of a manufactured object

- Aesthetic Design — 15 years;
- Functional Design — 10 years.

Copyright

- Computer Programs and Data — 50 years in South Africa

[1] some additional information can be found in the updated course slides, which have yet to make it into these notes

- Computer program's "author" is the person who exercised control over the making of the computer program.

Trade Secrets — not really property — the law protects industrial secrets

Trademarks forever!

Patents 20 years in South Africa, does not apply to software (yet)

5.1.1 Copyright

Copyright prevents others from copying original works without permission. It is granted for a limited time (50 years after death of author). It only protects the *expression* of an idea, and not the idea itself. There is often a fine distinction between the two. A copyrightable object must exist in a material form. In South Africa, copyright comes into being automatically and no registration is required.

In South Africa, computer programs are eligible for copyright, if they are original. So you would need permission for reproducing the computer program in any manner or form, or for making an adaptation of the computer program.

In general copyright infringement occurs where the copyrighted material of others is used for personal gain as opposed to private or personal use. Backup is allowed for personal use. Fair dealing is allowed for review, illustration in teaching, demonstration of equipment, ...

Copyright of programs lasts for 50 years after first made available to public — this is a very long time for software! The author of a computer program is the person who exercises control over the making of the program.

Exercise Discuss the main difference between software and literature. Apart from the constantly evolving nature of software, what else can you say about software that would make the literature analogy inappropriate?

5.1.2 Trade Secrecy

Laws governing trade secrecy vary from country to country. The central idea is to grant companies the right to keep certain kinds of information secret (e.g. a secret recipe), with the aim of allowing them to keep a competitive edge. The laws were not designed with computer technology in mind. In order for a piece of information to be considered trade secret, it must be possible to show that:

- It is novel
- Represents an economic investment to the claimant
- Has involved some effort in development
- The claimant has made some effort to keep it secret

Trace secrecy laws can be applied to software. This is usually done using non-disclosure clauses. Employees sign an agreement that they will not reveal secrets learnt at work even after they have left. There is often ambiguity here because the agreement does not apply to generic information in the area. Another application of this law is via licensing agreements. Software is licensed out and not sold – only the object code, and not the source code, is given to the user. The software company can do all the modification to suit the client and still retain control. The source code is in effect a trade secret.

5.1.3 Trademarks and Domains

Trademarks

Trademarks distinguishes one person's goods or services from those of another. The rights exist either via common law or by registration. Registered Trademarks are perpetually renewable in periods of 10 years [108, p. 243].

Domain Names

Domain Name System (DNS) is used instead of IP numbers. Generic Top Level Domain (gTLD) are ones such as .com, .net and .org + .aero; .biz; .coop; .info; .museum; .name; and .pro. (since 2000). This is all managed by ICANN (the Internet Corporation for Assigned Names and Numbers) which is a nonprofit organization responsible for the namespaces of the Internet.

The country code Top Level Domain (ccTLD) .za administered by `www.zadna.org.za`. The Internet Assigned Numbers Authority (IANA) is a department of ICANN, and coordinates the Internet Protocol (IP) addressing systems.

Cybersquatting Cybersquatting (or domain squatting), is when someone registers an Internet domain name in bad faith intending to profit from the good name of trademarks, famous people or businesses. The cybersquatter can then either sell the domain at an inflated price or use it to attract business.

Disputes are resolved by ICANN — Uniform Dispute Resolution Policy (UDRP), or .ZA Dispute Resolution Regulations (ZADRR)[2].

5.1.4 Patents

This is potentially the strongest form of protection because a patent

- Gives the inventor monopoly on the use of the invention – even if someone else makes the same product in a different way, they are excluded from using it;
- Grants patent owner the right to licence others to make, sell, or use the invention;

[2] `https://domaindisputes.co.za/`

- Legitimises a monopoly;
- Is granted for a limited number of years (20 in South Africa).

The main aim of the patents is not only to ensure the rights of the inventor, but also to advance useful arts and science. This will foster inventions and encourage others to learn from and build on inventions. It also promotes disclosure of inventions and assures that ideas already in the public domain remain there.

However, it must be noted that patent does not guarantee financial success. This is only achieved if the product is accepted by the market. Additionally one cannot patent an abstract idea, an algorithm or a scientific principle. To qualify for patent protection, the object in question must satisfy the following criteria:

- Falls into a category of permissible subject matter
- Satisfies the three tests of having utility, novelty, and non-obvious.

5.2 Scenarios

Pirated Software from Abroad

Bernie works for a large consulting company. When he was on holiday in South East Asia he found an Office suit that looks identical to Microsoft Office. The package he found costs R50 compared to the price tag of R3000 back home. Bernie knew that the seller does not honour US copyright law. Despite the documentation looking like it has been photocopied, he decided to buy it and returned home with it.

- Do you think Bernie has done anything wrong?
- Do you think the customs will confiscate it should they find out?

Stealing an Idea

It is 1980 and Bingo software has just developed a new operating system called BOS. BOS is better than anything else around but Bingo is a small firm and needed venture capital to start up. It spent 3 years bringing the product to the market, after which it launched and sold well for a year. At this point, it has recovered about 25% of initial investments. Pirate Pete entered the market with PPOS which is cheaper and has more features than BOS — but it appears to be a copied or slightly modified version of BOS. In addition to this, copying of BOS is rampant with customers making copies. Bingo did not last long and went bankrupt within a year.

- Do you think that this is unfair?
- Has PPOS wronged Bingo?
- Have the customers wronged Bingo?

In Bingo's case, trade secrecy would have helped. Non-disclosure agreements would prevent employee from giving away important secrets even after they left. However, this might only be useful during development; once BOS is released, it is more difficult to control. General principles are there for everyone to see (and copied) – BOS is trying to sell or licence the software, something just can not be hidden. However, specific behind-the-scene methods of doing something can still be made a secret. Generally, trade secrecy works for specialised bespoke software but is poor for general purpose software.

Improving Software

Earl develops a virus tester which is very good. It detects and repairs all known viruses. He makes the software and its source code available on the web for free and he also publishes an article on it. Jake reads the article and downloads a copy. He figures out how it works, downloads the source code and makes several changes to enhance it. After this, Jake sends Earl a copy of the modified software together with an explanation. Jake then puts a copy on the web, explains what he has done and gives appropriate credit to Earl.

- Discuss whether or not you think Earl or Jake has done anything wrong?

Exercise There are some issues that you should think about before proceeding further. Write down any thoughts you might have on each of the following:

- Distinction between hardware and software is often blurred.
- Macro issues — should software be owned? Should it be protected like property?
- Micro issues — are (unauthorised) copies illegal?
- Legal and moral issues — descriptive (what the law says) versus normative (what the law should say)

Protecting Software

Consider the Bingo scenario whereby PPOS copies BOS and sells it more cheaply. PPOS is able to do that because its development costs were lower. It also seems unfair that PPOS used BOS without paying. What is the solution to this problem? One is to give Bingo legal exclusive right to its software.

There are currently three mechanisms to deal with scenarios like Bingo: copyright, trade secrecy and patent.

5.3 Alternatives to Current Intellectual Property Regimes

In response to the misuse of current IP mechanisms to stifle, rather than encourage, creativity and innovation, a coherent movement has arisen to counteract it. Three different strategies are being deployed:

Open Source or Free Software: Freedom to use, study, modify and share software.

Open Content Freedom to use, study, modify and share scientific and creative works

Open Standards Publicly licensed standards that allow different hardware/software vendors to make products that interoperate

The central idea of the first two is to exploit the concept of IP, but instead to use it to guarantee to keep it open.

> **Open Source Software**
>
> *Open Source Software* is software of which the source code is publicly available. Its copyright holder provides people the rights to study, modify, and (re)distribute the code to anyone.

> **Open Source Software**
>
> *Free software* is software that is free (in the sense of liberty, not price). This means one has the freedom not just to run the software, but also copy, distribute, study, change and improve it. Free software is open source, but open source software is not necessarily also free.

In a play of words, this is also referred to as *copyleft*. It is a general method for making a program or other work free, and requiring all modified and extended versions of the program to be free as well. It uses copyright law, but flips it over to serve the opposite of its usual purpose: instead of privatising software, it becomes a means of keeping it free. Notably, under such rules, one can give everyone the permission to run the program, copy the program, modify the program, distribute modified versions, but not permission to add restrictions of their own. Thus, the crucial freedoms of "free" software are guaranteed to everyone who has a copy, and it cannot be taken away.

This can be put into a licensing model. So, then each open source project has a license associated with it that indicates what rights and responsibilities the user of the software has. A very common license is the GNU General Public License (GPL), which allows the user to:

- freely copy and distribute copies of source code and software, only with the license
- modify code, but those changes must be clear and made available with the same license

Other open licenses include BSD-Style Copyright and Mozilla Public License (MPL).

Popular, and widely used, open source software are, among others, Linux (and its derivatives, such as the Ubuntu operating system), Apache web server (most web serves in the world use it), database software such as PostgreSQL, and office suites such as OpenOffice.

Other fields observed the success of this copyleft notion and followed suit. The most popular one is the Creative Commons[3]. CC expands the range of creative work available to others legally to build upon and share. Key themes there are fairly similar to the open source

[3] `http://creativecommons.org`

software movement's ideas. It's about Sharing, Accessing, Collaborating and Negotiating, so as to unleash the potential of the digital environment to facilitate the "cut and paste", remix, P2P, with attribution and unencumbered by large transaction costs and threats of lawsuits. The four protocol components are:

Attribution Other people may use, modify and distribute the work, as long as they give the original author credit.

Non-commercial Other people may use, modify and distribute the work, but for non-commercial purposes only.

No derivatives Other people may use and distribute the work, but can not modify it to create derivative works.

Share alike Other people may modify the work and distribute derivatives, but only on the condition that the derivatives are made available to other people on the same licence terms. This term can not be used with the No Derivatives term, because it applies only to derivative works.

For each creative work, the creator chooses yes/no for each of them. For instance, these notes are now made available under a CC-BY licence, and there are several open textbooks[4], open access science journals, and linked open data. UCT also provides lots of open content, such as through OpenUCT[5] and other efforts, such as the Computer Science departmental server of publications, theses, and honours projects[6]. The, perhaps, most famous online open resource under a CC-BY licence is Wikipedia.

5.4 Fair Use in the Electronic Age

** *Note: this is an old section and is kept for historical purpose, for now. It most likely has been updated, and may differ from country to country.* **

The purpose of this section is to outline the lawful uses of copyrighted works by individuals, libraries, and educational institutions in the electronic environment. Representatives of the following associations advocate the arguments below:

American Association of Law Libraries, American Library Association, Association of Academic Health Sciences Library Directors, Association of Research Libraries, Medical Library Association and the Special Libraries Association.

"'The primary objective of copyright is not to reward the labour of authors, but "to promote the Progress of Science and useful Arts." To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work. This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art.' - US Supreme Court Justice Sandra Day O'Connor

[4] one of the open textbook libraries is available at `https://open.umn.edu/opentextbooks`.
[5] `https://open.uct.ac.za`
[6] `http://pubs.cs.uct.ac.za/`

It follows that the benefits of the new technologies should flow to the public as well as to copyright proprietors. As more information becomes available only in electronic formats, the public's legitimate right to use copyrighted material must be protected. In order for copyright to truly serve its purpose of "promoting progress," the public's right of fair use must continue in the electronic era, and these lawful uses of copyrighted works must be allowed without individual transaction fees.

Without infringing copyright, the public has a right to expect:

- to read, listen to, or view publicly marketed copyrighted material privately, on site or remotely
- to browse through publicly marketed copyrighted material
- to experiment with variations of copyrighted material for fair use purposes, while preserving the integrity of the original
- to make or have made for them a first generation copy for personal use of an article or other small part of a publicly marketed copyrighted work or a work in a library's collection for such purpose as study, scholarship, or research
- to make transitory copies if ephemeral or incidental to a lawful use and if retained only temporarily Without infringing copyright, non-profit libraries on behalf of their clientele, should be able:
- to use electronic technologies to preserve copyrighted materials in their collections
- to provide copyrighted materials as part of electronic reserve room service
- to provide copyrighted materials as part of electronic inter-library loan service
- to avoid liability, after posting appropriate copyright notices, for the unsupervised actions of their users

Users, libraries, and educational institutions have a right to expect:

- that the terms of licenses will not restrict fair use or other lawful library or educational uses
- that U.S. government works and other public domain materials will be readily available without restrictions and at a government price not exceeding the marginal cost of dissemination
- that rights of use for non-profit education apply in face-to-face teaching and in transmittal or broadcast to remote locations where educational institutions of the future must increasingly reach their students

Carefully constructed copyright guidelines and practices have emerged for the print environment to ensure that there is a balance between the rights of users and those of authors, publishers, and copyright owners. New understandings, developed by all stakeholders, will help to ensure that this balance is retained in a rapidly changing electronic environment. The above working statement addresses lawful uses of copyrighted works in both the print and electronic environments.

Chapter 6

Privacy and Civil Liberties

The word privacy is derived the Latin word *privatus*, and refers to the state of being free from unauthorised observation or intrusion [77]. There is no consensus on the definition of privacy within philosophy. There are generally two schools of thought, namely reductionism and coherentism. Reductionists argue that one cannot be entitled to a right to privacy because a right to privacy can be reduced to other fundamental issues of property and person [51]. These individuals are critical of privacy as a separate notion. Consider the example of a man who owns a picture they do not want to share with others [111]. This individual has a collection of positive and negative rights [111, p.288]. This means that they have the right to sell this picture to whomever, the right to destroy it, prevent others from doing certain things to it, etc. Any violation to his right of privacy, with respect to the picture, can be defined as a violation of the many rights he has over his property.

Thomson [111] argues that we should not be looking for a clear definition of privacy, as notions of privacy are derivative. Simple definitions of privacy such as being "left alone" [111, p.295] are insufficient. This is because they do not capture its fundamental boundaries, if one were to hit you with a brick on the head, they are not leaving you alone, however, they are not violating your right to privacy. We could not define privacy by attempting to find a specific thing which would be protected by a right.

There are also individuals who defend and believe there exists a notion of privacy. Unlike Thomson [111], they argue that even if the right to privacy is derivative (meaning all the collection of rights can be explained by means of other rights). That does not mean they do not all collectively point to an underlying issue [111]. Moreover, we may not be able to guarantee by privacy protections if we assume that property and personal rights can protect the unique unified issue [89].

Tavani [108] identifies and summarises three views on privacy, as follows (from its Table 5.1)

Accessibility privacy: One's physically being let alone, or being free from intrusion into one's physical space.

Decisional privacy: Freedom from interference in one's choices and decisions.

Informational privacy: Control over the flow of one's personal information, including the transfer and exchange of that information.

Can you find examples of each? What does the opposite of each one entail? For instance, one may experience diminished decisional privacy due to being prevented from seeking information on a particular topic or be policed on the search terms put in the search engine that would have a net results that you wouldn't search for information on that topic.

On privacy

"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Edward Snowden

There have been multiple arguments motivating why privacy is important. There is the argument it is important because it allows to protect our reputations and the secrecy of our matters [89, p.30]. This is not sufficient because individuals value privacy even if they knew that information collected about them would not be used for nefarious purposes [89]. Another argument is that it is values because without it we cannot form relationships. This view claims that intimacy in human relationships is possible because individuals have the ability to share information with others, and are able to withhold information from others. This view has been criticised for its lack of focus on the quality and intensity of relationships, and taking a market-like view on personal relationships [89]. In particular, the sharing of vast information between two individuals does not necessarily mean that the relationship is intimate. One's mental health professional, be it a social worker or psychologist, may be aware of much more information about an individual, however, that does not mean the relationship is anything but professional.

Privacy cannot also be defined based only on the principle of respect for others [89, p.36]. Reiman [89] argues that "privacy is a social ritual by means of which an individual's moral title to his existence is conferred. Privacy is an essential part of the complex social practice by means of which the social group recognizes – and communicates to the individual – that his existence is his own. And this is the a precondition of personhood" [89, p.39]

Big Brother

Big Brother is fictional character in George Orwell's book "1984" that is the leader of a totalitarian state and observes everyone constantly. It is now used as a general concept for abuse of power in the sphere of civil liberties and mass surveillance, be this by the government or other organisations, which is greatly facilitated by ICT.

6.1 Privacy and the Law

The current state of the world is that governments have tools that enable them collect information about civilians. The Mexican government, for instance, has been accused of using

spyware on journalists and activists who are working on exposing corruption and government's serious failures [2]. The infringement of citizens' privacy by governments may also be done through the cooperation of telecommunications companies [36].

Governments are not the only actors with the ability to commit such violations; civilians also have the capability of buying equipment from all over the world to enable the tracking of individuals. They also have methods for dissemination of information in an easy manner. A significant number of these abilities are a result of the existence of the Internet. The legal systems in countries have evolved in order to be better equipped to deal with such violations. South Africa's legal system has also had to evolve. Generally, the reference point for the protection of privacy has been the 1948 Universal Declaration of Human Rights [58]. However, not all countries had voted in favour of the declaration for various reasons. South Africa's legal system is of mixed nature, and its foundation is Roman-Dutch law [106].

The foundation for privacy laws in South Africa is the case O'Keeffe v Argus Printing and Publishing Co Ltd in 1954, where a journalist objected to the mass publication of her picture for the purpose of advertising, to which she did not consent [96]. The court ruled in her favour and stated that the newspaper "in a manner inconsistent with the decencies of life and in so doing they were guilty of an act for which there ought to be a legal remedy" [17, p.7]. Following the judgement, South African courts ruled against intrusions such as the placement of listening devices without a person's consent, listening in on private telephone conversations, unconsented blood tests, etc [17]. South African courts persisted to use the *actio iniuriarum* (regarding the infringements of rights regarding dignity, reputation, and physical integrity) as a source of protection of personality rights [17]. Moreover, one could not use the validity of a publication as defense in a case of defamation. One had to show that the publication was in the public good.

It is for these two reasons that South Africa had to develop specific laws around the issue of privacy [17]. The two existing acts are the *Regulation of Interception of Communications and Provision of Communication Information Act (RICA)* and the *Protection of Personal Information (POPI) Act*. Judges at the South African constitutional court have, at some point, defined privacy as the "right of a person to live his or her life as he or she pleases" [17, p.12]. In other words, the role of privacy legislation is to protect the personhood and autonomy of individuals.

The South African constitution, which was announced in 1996, states that everyone has the right to privacy, which includes the right *not* to have (1) their person or home searched, (2) their property searched (3) their possessions seized, or (4) the privacy of their communications infringed.

6.1.1 RICA

The act pertaining to the interception of electronic communications came into full effect in September 2005. RICA seeks to regulate the interaction of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information. In order to be able to monitor communication the following steps must be taken: (1) Law enforcement must be in possession of information or evident that electronic communications are being used in the commission of the crime, (2)

They must approach the court and request an "interception direction". The sitting judge will then decide on the merit of the evident present and will grant or refuse this directive, and (3) once the interception direction is obtained, it can then be served to the relevant service provider who is then required by law to monitor any communication made by the individual or party concerned and then to forward all surveillance information to the law enforcement agency. Note that the person under surveillance needs not be informed.

RICA provides that all forms of monitoring and interception of communications are unlawful unless the monitoring and interception takes place under one of the recognized exceptions in RICA. There are several exceptions to the general rule on the prohibition on intercepting communications, three of which apply to monitoring in the workplace.

Section 4 of the RICA allows a party to a communication to monitor and intercept the communication if he/she is a party to the communication (for example, where the participants in a meeting consent to the meeting being recorded). This exception also applies where the interceptor is acting with the consent of one of the parties to the communication.

Section 5 allows for interception of any communication under any circumstances, that is, no special motivation or reason is required for it provided the person whose communication is being intercepted has consented to it in writing prior to such interception. Section 6 contains a so-called "business purpose exception" which involves the interception of "indirect communications in connection with the carrying on of business". Section 6 authorises any person to intercept indirect communications in the course of carrying out their business by means of which a transaction is concluded in the course of that business, which "otherwise relates to that business" or which "otherwise takes place in the course of the carrying on of that business, in the course of its transmission over a telecommunication system".

6.1.2 POPI Act

The Protection of Personal Information Act (PoPI) sets conditions for how you can process information. It has been signed by the President and is law and is run by the "Information Regulator". In some sense this is a counterbalance to the Interception Act. This act seeks to provide South African with legal means to protect their personal information. As we have seen, it is also covered through the Constitution and a number of sections of other Acts. The act also deals with the rapid transfer of personal information with other countries via the internet and call centres, similar to the EU Global Data Protection Regulation (GDPR).

In South Africa, General Information Protection Principles (GIPP), applies to those who process personal information (generally, anyone with customers, partners or staff who store their personal information in some way)

- Collect only information needed for a specific purpose;
- Apply reasonable security measures to protect information;
- Ensure such security measures are relevant and up-to-date;
- Only hold as much information as needed;
- Only hold information for as long as it is needed; and

- Allow the subject of the information to view it upon request.
- If information is transferred across borders must ensure compliance with the restrictions in terms of the PoPI Act (similar to EU)
- If information is used for direct marketing the data subject has to give his or her consent or be a customer

The EU Global Data Protection Regulation (GDPR)[1] was approved in April 2016, and officially enforced from 25 May 2018. This has been a major policy change intended to harmonise the data privacy laws throughout Europe. In addition to the material covered in this chapter, you should familiarise yourself with the key aspects of this regulation, which can be found at eugdpr.org. It applies to all processing of personal data, including data of EU citizens being handled outside of the EU (e.g., in South Africa). Request for consent must be given in intelligible and easily accessible form, with clear communication of the purpose for the processing. Data subject rights have been increased, including the right to be forgotten, and data portability. Data privacy should also be considered from the onset of designing systems rather than being added later.

On the other side of the issue, as much as government regulation is used to protect privacy, there has also been pressure on companies to release private data to governments.

Example 6.1: Back door access to a smartphone, or not.

> On Dec 2015, a married couple committed a mass shooting in California, United States of America. The police and other authorities were able to recover one of the suspects' phone, an iPhone whose security features had been enabled. The following year, the Federal Bureau of Investigation (FBI) approached Apple Inc, the manufacturer of the phone. Their goal was to use the courts to compel the company to create a special version of their operating system that would allow them to circumvent the security features [97]. This was met with resistance by the company and sparked numerous debates. The company opposed the FBI's request stating that "it was wrong and would set a dangerous precedent" [130]. Eventually, the FBI were able to unlock the phone without help from Apple [130].

Encryption in case of the phone is used to provide the owner with privacy. It may seem only reasonable, at first glance, to expect Apple to 'provide' the FBI with a backdoor to the iPhone thus bypass all security features. It is not possible to give law enforcement agencies such as the FBI a backdoor without compromising encryption and therefore privacy [94], because creation of backdoors for law enforcement agencies creates a possibility for malicious actors to also exploit such backdoors.

[1] `https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en`

More information on the PoPI Act can be found in the act itself[2]

6.1.3 Privacy across the globe?

Besides the South African constitution, RICA and the POPI Act, there are other laws on privacy that affects anyone to a greater or lesser extent. A continental view and assessment on data privacy laws in Africa can be found in the collection edited by A.B. Makulilo [72].

Why consider laws in other countries than the one where you live? The internet is a *global* network of computers. This causes some issues of jurisdiction of regulations. For instance, your UCT student emails are stored in Microsoft's cloud somewhere in the world, the servers with the actual email storage are probably those located in their data centre Dublin in Ireland (part of the European Union), whereas Microsoft as organisation is registered in the USA. Whose privacy rules apply? Those from South Africa, Ireland, the EU, or the USA?

At the world-wide scale, there is clearly a policy vacuum as well as conflict, which is not set to be the lowest common denominator. The main differences on principle are the *laissez faire* and intrusion approaches to privacy in the USA vs the increased amounts privacy protection regulations in the EU, where both try increase their level of influence. Failing that, companies are realising that there is a sizeable number of clients who do care about privacy, and accordingly set up their own principles. For instance, Microsoft's "Six Principles for International Agreements Governing Law Enforcement Access to Data" and Dropbox has a similar list as well (in 2018 at least).

There is a further dimension of *trust*, or the lack thereof, both politically between countries and due to technological sophistication. A recent and, at the time of writing still ongoing, case is that of Huawei, a Chinese IT company of which the US government says that their new technologies could be used to spy on US citizens and therewith compromising national security. Huawei vehemently denies this. Conversely, as hypothetical example, let's say that the South African government falls out of favour with the US government at the end of the year such that companies have to cease to do business in South Africa, provide no services to South Africans, and the FBI would get search warrants over the data. You would lose access to your UCT emails, Gmail, Dropbox, Github, Facebook, WhatsApp etc. etc., and all that data and usage statistics you have given those companies are fair game to them to analyse as they please[3]. Should that data perhaps be stored in South Africa instead, just in case? Is there, or should there be, such thing as *ICT sovereignty*?

6.2 Privacy and technology

While much more can be said about privacy in general (see also, e.g., [28] for a philosophical account), as well as principles of privacy and IT [53], in this section we shall look a more practical aspects to sensitise you to concrete issues and to start analysing them.

[2] `http://www.gov.za/documents/protection-personal-information-act`

[3] Then, there is the physical infrastructure of the cables and servers. Do you know who owns the Seacom cable?

6.2.1 Data sharing

There are technologies which enable companies to be able to collect large amounts of data about our use of the products. The tracking of online activity is generally not created for malicious reasons. Online stores track the products we buy, view, and search. This is done to improve their services and enable them to advertise based on personalised data, among other things. This data is often stored and transferred between a companies' data centers. This create the possibility of actors to intercept this data and use it for other reasons. The British Government's Communications Headquarters (GCHQ) and the USA's National Security Agency were guilty of committing such a violation with their Muscular project that intercepted communications between Google's data centers [39]. These companies make use of powerful computers with the ability to store and process large amounts of data. There is reason to believe that even if data were 'privatised', it is still possible to discover the underlying identities. There are researchers who have shown that even if the personal identity data such as names and addresses, it is still possible to identify individuals based on a few credit-card transactions [30].

The use of surveillance systems by governments also has an additional ethical problem. Governments may exploit faults in smart-phones, smart TVs, and other technologies when building modern surveillance systems. This means that they have an incentive to not report issues they discover. Unfortunately, when they lose control of their tools (recently, tools have been stolen from the NSA [88]), they open the floodgates to more malicious actors who intend to infringe people's privacy.

Example 6.2: Scenario: Using data for different things.

> If we consider the case of an individual named Ravi, who works for a credit card company, developing new products. Ravi gains an interest in data mining and convinces his supervisor to buy a tool to analyse their data. With this tool, Ravi can get information on customers' buying habits, as well as finds out a correlation with postal codes to loan defaults. Based on this new information, a new policy can be formulated resulting in his company refusing credits to clients in 'bad' postal code areas. Doing this could reduce his company's exposure to bad loans. Ravi also discovers that Zoroastrians who donate to charity charges a substantial amount to their credit cards. He promptly recommends a new policy of soliciting more Zoroastrians for credit card in hope of increasing his company's profit. Here we see that the same data that can be used to improve our user experience can also be used in other ways. Are either of these two recommendations wrong? What about the way Ravi uses this information? Is the company wrong by implementing such policies?

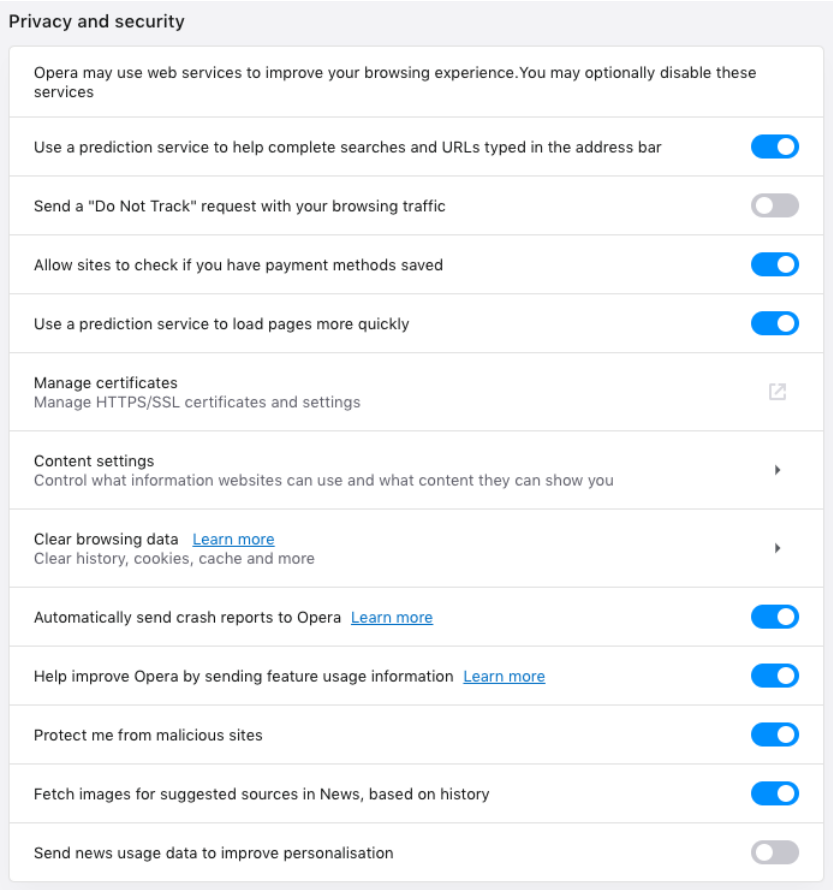

Figure 6.1: Screenshot of the default settings in a new installation of the Opera browser. By default it allows privacy invasions, such as saved payment methods and which features of the browser you are using (i.e., it monitors your behaviour). These are common default settings also for other browsers and software.

6.2.2 Browser Software and Cookies

Protecting one's privacy in the digital age is often difficult. The Electronic Frontier Foundation (EFF), an organisation that protects and champions individual's rights to privacy in the digital age, advocate a number of strategies for protecting one's privacy. One may be "shedding" personal details, including e-mail addresses and other contact information, without even knowing it unless they properly configure their Web browser; check, e.g., your browser's "Setup", "Options" or "Preferences" menus. Also be on the lookout for system wide "Internet defaults" programs on your computer; an example of such 'default setting' is shown in Figure 6.1: by default, the software will communicate with the software supplier, sending it various information on your usage of the tool. While some settings are useful for various things, you may not wish to enable them all.

Further, households with children may have an additional security problem – have you set clear rules for your children, so that they know not to reveal personal information unless you OK it on a site-by-site basis?

Cookies are a small amount of information that Web sites store on your computer, tempor-

Figure 6.2: Screenshots of three cookie messages, with different descriptions on what they do with the data and how to entice you to say "yes" to the cookies.

arily or more-or-less permanently. In many cases, cookies are useful and innocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for data mining purposes, to track your motions through a Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands.) It is unknown whether all of these cookie rings (some examples of which are Double Click and Link Exchange) do in fact share user data, but they certainly can do so potentially.

Browsers enable users to have some control over cookies, such as accepting them and deleting the stored cookies. Both EU legislation and South African law (PoPI) require website to ask the visitor to accept cookies and to state what the cookie data is used for (see

Figure 6.2), although this is more strictly enforced in the EU than in South Africa.

6.2.3 Privacy in the cloud

The 'cloud' is basically a whole bunch of servers and storage disks that present themselves to the user as if it's only one entity. Those devices are physically located at one or more sites in so-called *data centres*. Most organisations providing such cloud-based services have only a few data centres across the globe, thus, we walk into transnational privacy law issues again, as mentioned in Section 6.1.3.

What privacy do you have there? To illustrate, the Apple iCloud terms of use[4] state that "Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, *and may pre-screen, move, refuse, modify and/or remove Content at any time*, without prior notice and *in its sole discretion*, if such Content is found to be in violation of this Agreement *or is otherwise objectionable*." (emphasis added) or, in layperson's terms: they can do with your data whatever they want and look into it as much as they like. That is: there is no information privacy. MS Office 365 and OneDrive terms are alike Apple's iCloud terms of use. Especially 'free' (at no monetary cost) cloud-based services are similar, with specific usages, such as Gmail analysing email text automatically to, among others, tailor advertising[5]. Amazon's digital assistant Alexa stores every utterance in its cloud for better voice analysis.

What mitigation options or alternatives are there? For the likes of Gmail+Google and Live.com+Bing, i.e., email from the same organisation that you use as search engine: log out of the email and of the account before searching the web, lest you get stuck in that filter bubble. Alternatively, use a free email account from one company and the search engine of another. For storage providers of files, the issues are less easy to circumvent and the guaranteed safe alternative is carrying around external storage (disk, USB drive).

6.2.4 Paying with your privacy

User have become used to the idea that information and apps from the web are, or ought to be, 'for free' and they have become used to getting 'good deals' and reductions on products in, say, the supermarket. For instance, one does not have to pay for using a search engine, read the news online, download games, install chat software on the smartphone, etc. But in most cases, someone has paid for the development of the tools and infrastructure provided by those companies, and somehow do make profit anyhow. The typical business model is to exploit the data you give them about yourself, so that they can improve advertisement (those advertisers pay those companies) or can sell your data onward to other companies on the data market. We have seen some examples of desktop apps and the customer loyalty cards, but it also easily extends into the smartphone sphere. More than 70% of mobile apps report personal data to tracking companies [115], such as Google Analytics and FB Graph API, effectively having created a "smartphone panopticon"[6]

[4] `https://www.apple.com/legal/internet-services/icloud/en/terms.html`; last accessed Oct 17, 2018.
[5] `https://policies.google.com/terms`; last accessed on Oct 17, 2018
[6] You can check mobile apps and their trackers at `https://www.haystack.mobi/panopticon/`.

Essentially, the currency you pay in for using those 'free' services, is data about yourself. That is, the services are *not* for free, it's just that you don't pay for them with money. Consider again Figure 6.2 and especially the first cookie message of AccuWeather: you can avoid tracking and privacy intrusion by paying for the service with money (button on the right) or do not pay money and be tracked (button on the left). Reflecting on this (not uncommon) approach: this amounts to putting a monetary value on privacy. Is privacy really 'for sale'? Is a piece of your data as valuable as the money they can make from it, or should that be regulated? Beyond such practical questions lurks the more thorny issue in that the poor either have to 'sell themselves' or forfeit the service, whereas the rich can buy themselves their privacy. Is this rich/poor divide on privacy ethical? Is it enshrined in the constitution or other state laws that the privacy should be the same for everyone? If so, can those companies be held to account; if not, should there be such a law?

Other

Here are some other do's and don'ts, which may be a bit dated by the time you read this.

The speed of the Internet is often reflected in rapid online acquaintances and friendships. But it is important to realise that you don't really know who these people are or what they are like in real life. A thousand miles away, you don't have friends of friends or other references about this person. Be also wary of face-to-face meetings. If you and your new online friend wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn't be paranoid, but one should not be an easy mark, either. Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn't reveal this page to everyone you meet in a chat room.) For this and other reasons, many people maintain two personal home pages, a work related one, and an "off duty" version. Realise you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer. In most countries (including South Africa), employees have little if any privacy protection from monitoring by employers. When discussing sensitive matters in e-mail or other online media, be certain who you are talking you. If you replied to a mailing list post, check the headers – is your reply going to the person you think it is, or to the whole list? Also be aware that an increasing number of employers are monitoring and recording employee Web usage, as well as email. This could compromise home banking passwords and other sensitive information. Keep private data and private Net usage private, at home.

There's a high probability that "the system" is gathering this information for direct marketing purposes. In many cases your name and address are worth much more to them (because they can sell it to other marketers, who can do the same again - a snowball effect) than what you are (supposedly) getting from them. Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

Spam, or unsolicited bulk e-mail, is something you are probably already familiar with (and tired of). If you get a spammed advertisement, certainly don't take the sender up on whatever offer they are making, but also don't bother replying with "REMOVE" in the subject line, or whatever (probably bogus) unsubscribe instructions you've been given). This simply confirms that your address is being read by a real person, and you'll find yourself on dozens more spammer's lists in no time. If you open the message, watch your outgoing mail queue to make sure that a "return receipt" message was not generated, to be sent back to the spammer automatically. (It is best to queue your mail and send manually, rather than send immediately, so that you can see what's about to go out before it's actually sent.) If you have a good Internet service provider, you may be able to forward copies of spam e-mail to the system administrators. They can route a complaint to the ISP of the spammer (or if you know a lot about mail headers and DNS tools, you can probably contact these ISPs yourself to complain about the spammer.)

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a "side" account some pseudonymous or simply alternate address, and to use your main or preferred address only on small members-only lists and with known, trusted individuals. Addresses that are posted (even as part of message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public "throw away" address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your "real" address. You can use a free (advertising supported) e-mail service provider like Google or Live.com or Yandex for such "side" accounts. It is best to use a "real" Internet service provider for your main account, and to examine their privacy policies and terms of service, as some "free mail" services may have poor privacy track records. You may find it works best to use an e-mail package that allows multiple user IDs and addresses (i.e. "personalities", "aliases") so that you do not have to switch between multiple programs to manage and use more than one e-mail address

Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted). In Firefox, look for a closed lock (Windows) or unbroken key (Mac) icon at the bottom of the browser window. In Internet Explorer, look for a closed lock icon at the bottom (Windows) or near the top (Mac) of the browser window. In any browser, look at the URL (Web address) line – a secure connection will begin `https://` instead of `http://`. If you are at page that asks for such information but shows `http://`, then try adding the `s` yourself and reload the page. If you get an error message that the page or site does not exist, then don't send your data.

Last but certainly not least, there are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include industrial espionage, government surveillance, identity theft, disgruntled former associates, and system crackers. Relatively easy to use e-mail and file encryption software is available for free, such as Pretty Good Privacy (PGP), which runs on almost all computers and even integrates seamlessly with most major e-mail software. Good encryption uses very robust secret codes, which are difficult if not impossible to crack, to protect your data. You can also use a virtual private network (VPN), which can completely disguise to Web sites where you are coming from and who you are (and block all cookies).

6.3 Freedom of expression

Freedom of expression is a class of rights that exists so that individuals are able to make their opinions heard, and hear the opinion of others [8]. This freedom is characteristic of democracies. It generally extends to numerous forms of expression. Films, books, expressions by actions such as vigils, burning a flag, etc are all generally protected [8].

Expression can also be offensive, and may result in reputational injury, etc [25]. In particular, consider the case when one expresses themselves about a certain topic through the use of flyers. This will obviously result in littering that will have to cleaned by municipal workers (thus it costs the taxpayer). These are among the reasons why freedom of expression has limitations. Generally, its limitations are for preventing the infringing of other important rights [105]. Other examples are that denying the Holocaust is a crime in Germany, one should not insult the Dutch King in the Netherlands, and some presidents of countries are not to be defamed. How such laws would be enforceable across borders and, say, on some online social media platform of a company that has its headquarters in another country, is still being worked out.

The nature of Internet also results in quandaries about freedom of expression, some of them pre-date the Internet, but have been exacerbated by it. The Internet allows individuals to cheaply distribute content (and opinions) at a low cost. It also makes it easier for individuals to obtain, edit, and redistribute it. Moreover, it is makes it possible to send and receive information from a diverse and global audience. The sheer volume that one has access to also requires one to be able to organise this information [7]. It has worsened the conflict between advocates of intellectual property and freedom of expression. In particular, Internet users now have platforms to which discuss and share fan art. Furthermore, they can easily sell their fan art which can be considered an expression. Unfortunately, it often a violation of existing intellectual property laws. Works that are produced by supporters of certain products have long existed. They have been tolerated because only "a few people wrote fan fiction on their typewriters, made jokes about trademarked elements in casual conversation or in limited geographic areas, or made the occasional copy of a record on their cassette tape recorder" [pg.15, 18]. Unfortunately, the Internet has made it possible for individuals to distribute copyrighted materials at a low cost and be able to cost the copyright owners a significant amount of financial loss. Furthermore, private companies that own ISPs (and other telecoms companies) may silence certain individuals' 'expression' in order to increase the profits of their advertising partners. They may not be censoring ideas they do not agree with or like, but may only be diverting user's attention to 'expressions' which have a financial benefit for them. The South African government prevents the latter problem through its support for net neutrality, the view that all data that travels through an ISPs network should be treated equally [84].

6.4 Privacy and Ubuntu

Ubuntu is a broader community-based mindset, whereas privacy arises in a tradition with a strong emphasis on the rights of the individual in order to protect and empower them. Ubuntu has less of a concept of privacy — leaves a vacuum in this regard. At the same -

at the core of privacy is the call to protect dignity, which is in harmony with ubuntu. The South African Constitution (1996) enshrines the right to privacy as a constitutional right. See "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa" by Olinger, Britz and Olivier.

Bibliography

[1] A. Acquier, T. Daudigeos and J. Pinkse, 'Promises and paradoxes of the sharing economy: an organizing framework', *Technological Forecasting and Social Change*, vol. 125, pp. 1–10, 2017, ISSN: 0040-1625.

[2] D. Agren, *Mexico accused of spying on journalists and activists using cellphone malware*, Accessed: 20 June 2017, Jun. 2017. [Online]. Available: https://www.theguardian.com/world/2017/jun/19/mexico-cellphone-software-spying-journalists-activists.

[3] Al Jazeera News, *Cameroon shuts down Internet in english-speaking areas*, 2017. [Online]. Available: http://www.aljazeera.com/news/2017/01/cameroon-anglophone-areas-suffer-internet-blackout-170125174215077.html (visited on 25/04/2017).

[4] S. Allison, 'Hey google, our breasts aren't sexual', *Mail & Guardian*, Dec. 2017, Last accessed: 4 May 2019. [Online]. Available: https://mg.co.za/article/2017-10-12-hey-google-my-breasts-are-not-inappropriate.

[5] C. Arthur, *How low-paid workers at 'click farms' create appearance of online popularity*, 2013. [Online]. Available: https://www.theguardian.com/technology/2013/aug/02/click-farms-appearance-online-popularity (visited on 25/04/2017).

[6] D. H. Autor, 'Why are there still so many jobs? the history and future of workplace automation', *Journal of Economic Perspectives*, vol. 29, no. 3, pp. 3–30, 2015.

[7] J. M. Balkin, 'Digital speech and democratic culture: a theory of freedom of expression for the information society', *NYUL rev.*, vol. 79, p. 1, 2004.

[8] A. Barak, 'Freedom of expression and its limitations', *Kesher*, 4e–11e, 1990.

[9] R. N. Barger, *In search of a common rationale for computer ethics*, https://www3.nd.edu/~rbarger/common-rat.html, Accessed: 17-08-08, Apr. 1994.

[10] ——, *The Ross-Barger philosophy inventory*, https://www3.nd.edu/~rbarger/ross-barger, Accessed: 17-08-08, 1999.

[11] BBC Africa, *Why has Cameroon blocked the Internet?*, 2017. [Online]. Available: http://www.bbc.com/news/world-africa-38895541 (visited on 25/04/2017).

[12] BBC World Service, *Would you kill the big guy?*, http://www.bbc.co.uk/programmes/p00c1sw2, Accessed: 17-08-04, Nov. 2010.

[13] H. Berghel, 'Net neutrality vs. net neutering', *IEEE Computer*, pp. 73–77, Mar. 2016.

[14] J. E. Bessen, 'How computer automation affects occupations: technology, jobs, and skills', Boston Univ. School of Law, Law and Economics Research Paper No. 15-49, Oct. 2016.

[15] J.-F. Bonnefon, A. Shariff and I. Rahwan, 'The social dilemma of autonomous vehicles', *Science*, vol. 352, no. 6293, pp. 1573–1576, 2016.

[16] B. Bujo, 'Is there a specific African ethic? towards a discussion with western thought', in *African Ethics: An Anthology of Comparative and Applied Ethics*, M. F. Murove, Ed., University of Kwazulu-Natal Press, 2009, ch. 7, pp. 113–128, ISBN: 9781869141745.

[17] J. Burchell, 'The legal protection of privacy in South Africa: a transplantable hybrid', *Electron J Comp Law*, vol. 13, no. 1, 2009.

[18] Business Report, *MTN Cameroon asked to block Twitter*, 2011. [Online]. Available: http://www.iol.co.za/business-report/technology/mtn-cameroon-asked-to-block-twitter-1043582 (visited on 25/04/2017).

[19] Cameroon Online, *Cameroon's Internet outage is draining its economy*, 2017. [Online]. Available: http://www.cameroononline.org/cameroons-internet-outage-draining-economy/ (visited on 25/04/2017).

[20] M. Castells, *The power of identity: The information Age: Economy, society and culture, Volume II (The information age)*. Wiley-Blackwell, 2003.

[21] ——, *The rise of the network society: The information age: Economy, society, and culture*. John Wiley & Sons, 2010, vol. 1, ISBN: 9781444319514.

[22] CERN, *The birth of the web*, http://cds.cern.ch/record/1998446, Accessed: 2017-08-03, Dec. 2013.

[23] T. Chengeta, 'Dignity, ubuntu, humanity and autonomous weapon systems (aws) debate: an african perspective', *Brazilian Journal of International Law*, vol. 13, pp. 460–501, 2016.

[24] CNNMoney, *Volkswagen scandal...in two minutes*, http://money.cnn.com/2015/09/28/news/companies/volkswagen-scandal-two-minutes/, Accessed: 17-08-04, Nov. 2015.

[25] J. Cohen, 'Freedom of expression', *Philosophy & Public Affairs*, pp. 207–263, 1993.

[26] D. Cole, *'we kill people based on metadata'*, 2014. [Online]. Available: http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/ (visited on 25/04/2017).

[27] J. Crowcroft, 'Net neutrality: the technical side of the debate: a white paper', *SIGCOMM*, vol. 37, no. 1, pp. 49–56, 2007.

[28] J. DeCew, 'Privacy', in *The Stanford Encyclopedia of Philosophy (Spring 2015 Edition)*, E. N. Zalta, Ed., 2015. [Online]. Available: http://plato.stanford.edu/archives/spr2015/entries/privacy/.

[29] M. Del Barco, *How Kodak's shirley cards set photography's skin-tone standard*, 2014. [Online]. Available: http://www.npr.org/2014/11/13/363517842/for-decades-kodak-s-shirley-cards-set-photography-s-skin-tone-standard (visited on 25/04/2017).

[30] B. Deng, *People identified through credit-card use alone*, http://www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817#/b2, Accessed: 20 June 2017.

[31] K. Dobransky and E. Hargittai, 'The disability divide in Internet access and use', *Information, Communication & Society*, vol. 9, no. 3, pp. 313–334, 2006.

[32] R. J. Domanski, *Who Governs the Internet?: A Political Architecture*. Lexington Books, 2015.

[33] Y. Dror, 'Values and the law', *The Antioch Review*, vol. 17, no. 4, pp. 440–454, 1957.

[34] B. Duggan, *Uganda shuts down social media; candidates arrested on election day*, 2016. [Online]. Available: http://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/index.html (visited on 25/04/2017).

[35] D. Edmonds, *Would you kill the fat man?: The trolley problem and what your answer tells us about right and wrong*. Princeton University Press, 2013.

[36] Electronic Frontier Foundation, *Nsa spying*, https://www.eff.org/nsa-spying, Accessed: 20 June 2017.

[37] P. Finn and S. Horwitz, *U.s. charges snowden with espionage*, https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html, Accessed: 2017-06-26.

[38] G. F. Gaus, *Value and justification: The foundations of liberal theory*. Cambridge University Press, 1990.

[39] B. Gellman and A. Soltani, *Nsa 'hacked google and yahoo's data centre links', snowden documents say*, http://www.independent.co.uk/news/world/americas/nsa-hacked-google-and-yahoo-s-data-centre-links-snowden-documents-say-8913998.html, Accessed: 20 June 2017.

[40] D. Gershgorn, 'Police used bomb disposal robot to kill a dallas shooting suspect', *Popular Science*, vol. 8 July, 2016, 2016. [Online]. Available: http://www.popsci.com/police-used-bomb-disposal-robot-to-kill-dallas-shooting-suspect.

[41] A. Goldstuck, *Social media now indispensable to sa brands*, http://www.worldwideworx.com/social-media-indispensable-sa-brands-2017/, Accessed: 2017-08-03, Sep. 2016.

[42] ——, *SA Internet penetration to reach 40% in 2017*, http://www.worldwideworx.com/internet2017/, Accessed: 2017-08-03, Jul. 2017.

[43] S. Golkar, 'Liberation or suppression technologies? the Internet, the Green Movement and the regime in iran', *International Journal of Emerging Technologies and Society*, vol. 9, no. 1, p. 50, 2011.

[44] Google, *Google code of conduct*, https://abc.xyz/investor/other/google-code-of-conduct.html, Accessed: 17-08-12, Aug. 2017.

[45] D. Gotterbarn, 'Computer Ethics- Responsibility Regained', *National Forum*, vol. 71, no. 3, p. 26, 1991. [Online]. Available: http://csciwww.etsu.edu/gotterbarn/artpp1.htm.

[46] T. Govier, *A practical study of argument*. Cengage Learning, 2010.

[47] G. Greenwald, E. MacAskill and L. Poitras, *Edward snowden: the whistleblower behind the nsa surveillance revelations*, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, Accessed: 2017-06-26.

[48] D. Harvey, 'Seventeen contradictions and the end of capitalism', in. London: Profile Books, 2014, ch. Technology, work and human disposability, pp. 111–121.

[49] U. S. Henama and P. P. S. Sifolo, 'Uber: the South Africa experience', *African ournal of Hospitality, Tourism and Leisure*, vol. 6, no. 2, 10p, 2017.

[50] R. Herschel and V. M. Miori, 'Ethics & big data', *Technology in Society*, vol. 49, pp. 31–36, 2017.

[51] S. Hongladarom, 'A buddhist theory of privacy', in *A Buddhist Theory of Privacy*, Springer, 2016, pp. 57–84.

[52] R. Hotten, *Volkswagen: the scandal explained*, http://www.bbc.com/news/business-34324772, Accessed: 17-08-04, Dec. 2015.

[53] J. van den Hoven, M. Blaauw, W. Pieters and M. Warnier, 'Privacy and information technology', in *The Stanford Encyclopedia of Philosophy (Summer 2018 Edition)*, E. N. Zalta, Ed., 2014. [Online]. Available: https://plato.stanford.edu/archives/sum2018/entries/it-privacy/.

[54] C. Huff and J. Cooper, 'Sex bias in educational software: the effect of designers' stereotypes on the software they design', *Journal of Applied Social Psychology*, vol. 17, no. 6, pp. 519–532, 1987.

[55] R. Hursthouse and G. Pettigrove, 'Virtue ethics', in *Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., Winter 2016 Edition, Accessed: 17-08-11, Metaphysics Research Lab, Stanford University, Dec. 2016. [Online]. Available: https://plato.stanford.edu/entries/ethics-virtue/.

[56] IITPSA, *Public recourse*, https://www.iitpsa.org.za/public-recourse/, Accessed: 17-08-04.

[57] S. Inskeep, *China's 'gold farmers' play a grim game*, 2007. [Online]. Available: http://www.npr.org/templates/story/story.php?storyId=10165824 (visited on 25/04/2017).

[58] Internet Service Providers' Association, *Right to privacy*, http://old.ispa.org.za/regcom/privacyfiles/chapter-2-righttoprivacy.pdf, Accessed: 20 June 2017.

[59] D. G. Johnson, 'Computer ethics', in *The Blackwell guide to the philosophy of computing and information*, ser. Blackwell philosophy guides, L. Floridi, Ed., Malden, MA: Blackwell Pub, 2004, ch. 5, pp. 65–75, ISBN: 978-0-631-22918-6.

[60] E. A. Kallman and J. P. Grillo, *Ethical Decision Making and Information Technology: An Introduction with Cases*, 2nd. DIANE Publishing Company, 1998, ISBN: 0788157205.

[61] I. Kant, 'On a supposed right to lie from altruistic motives', *Critical of practical reason and other writings*, pp. 346–350, 1949. [Online]. Available: https://www.unc.edu/courses/2009spring/plcy/240/001/Kant.pdf.

[62] J. E. Katz, *Magic in the air: Mobile communication and the transformation of social life*. Transaction Publishers, 2011, vol. 1.

[63] C. M. Keet, 'Dirty wars, databases, and indices', *Peace & Conflict Review*, vol. 4, no. 1, pp. 75–78, 2009. [Online]. Available: http://www.review.upeace.org/index.cfm?opcion=0&ejemplar=18&entrada=94.

[64] S. Kemp, *Digital in 2017: global overview*, https://wearesocial.com/special-reports/digital-in-2017-global-overview, Accessed: 17-08-04, Jan. 2017.

[65] M. Lawrie, *The history of the internet in south africa: how it began*, http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf, Accessed: 17-08-08, 1997.

[66] S. Lazar and C. Klein, 'Why we need more than just data to create ethical driverless cars', *The Conversation*, Oct. 2018. [Online]. Available: https://theconversation.com/amp/why-we-need-more-than-just-data-to-create-ethical-driverless-cars-105650.

[67] J. Lee, B. Bagheri and H.-A. Kao, 'A cyber-physical systems architecture for industry 4.0-based manufacturing systems', *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.

[68] S. Levin, *Uber launches 'urgent investigation' into sexual harassment claims*, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/feb/20/uber-urgent-investigation-sexual-harassment-claims-susan-fowler (visited on 01/05/2017).

[69] ——, *Uber manager told female engineer that 'sexism is systemic in tech*, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/mar/24/uber-manager-sexism-systemic-tech-kamilah-taylor (visited on 01/05/2017).

[70] D. Lindsay, *A list of fallacious arguments*, http://www.don-lindsay-archive.org/skeptic/arguments.html, Accessed: 17-08-04, Sep. 2013.

[71] M. C. Loui and K. W. Miller, 'Ethics and professional responsibility in computing', *Wiley Encyclopedia of Computer Science and Engineering*, 2008.

[72] A. Makulilo, Ed., *African Data Privacy Laws*. Springer, 2016.

[73] K. Malunga, 'Whistle-blowing in South Africa', Public Protector South Africa, Tech. Rep., Jan. 2015, Accessed: 17-08-04. [Online]. Available: http://www.pprotect.org/news/Whistle-blowing%20in%20South%20Africa27%20Jan%202015.pdf.

[74] M. Mamabolo, *Appeal looming in signal jamming court case*, http://www.htxt.co.za/2015/06/03/appeal-looming-in-signal-jamming-court-case/, Accessed: 17-08-04, Jun. 2015.

[75] G. Marchionini, H. Samet and L. Brandt, 'Digital government', *Communications of the ACM*, vol. 46, no. 1, pp. 25–27, 2003.

[76] J. S. Mbiti, *African Religions and Philosophy*, 2nd. Heinemann, 1990.

[77] Merriam-Webster Dictionary, *Definition of privacy*, https://www.merriam-webster.com/dictionary/privacy, Accessed: 20 June 2017.

[78] T. Metz, 'Toward an African moral theory', *Journal of Political Philosophy*, vol. 15, no. 3, pp. 321–341, Sep. 2007.

[79] T. Metz and J. B. Gaie, 'The African ethic of Ubuntu/Botho: implications for research on morality', *Journal of Moral Education*, vol. 39, no. 3, pp. 273–290, Sep. 2010. DOI: 10.1080/03057240.2010.497609. [Online]. Available: http://www.tandfonline.com/doi/full/10.1080/03057240.2010.497609.

[80] J. H. Moor, 'What is computer ethics?', *Metaphilosophy*, vol. 16, no. 4, pp. 266–275, 1985. (visited on 07/08/2017).

[81] ——, 'If Aristotle were a computing professional', *ACM SIGCAS Computers and Society*, vol. 28, no. 3, pp. 13–16, Sep. 1998.

[82] S. Moyn, *Rights vs. duties: reclaiming civic balance*, http://bostonreview.net/books-ideas/samuel-moyn-rights-duties, Accessed: 17-08-12, May 2016.

[83] M. Murthy, 'Facebook is misleading Indians with its full-page ads about free basics', *The Wire*, 26 December 2015 2015. [Online]. Available: http://thewire.in/17971/facebook-is-misleading-indians-with-its-full-page-ads-about-free-basics/.

[84] MyBroadband, *Net neutrality in South Africa must be protected: ispa*, https://mybroadband.co.za/news/internet/163492-net-neutrality-in-south-africa-must-be-protected-ispa.html, Accessed: 20 June 2017.

[85] J. E. O'Neill, 'The role of ARPA in the development of the ARPANET, 1961-1972', *IEEE Annals of the History of Computing*, vol. 17, no. 4, pp. 76–81, 1995, ISSN: 1058-6180. DOI: 10.1109/85.477437.

[86] C.-S. Ong, S.-C. Chang and C.-C. Wang, 'Comparative loneliness of users versus non-users of online chatting', *Cyberpsychology, Behavior, and Social Networking*, vol. 14, no. 1-2, pp. 35–40, 2011.

[87] L. Penny, *Robots are racist and sexist. just like the people who created them*, 2017. [Online]. Available: https://www.theguardian.com/commentisfree/2017/apr/20/robots-racist-sexist-people-machines-ai-language (visited on 25/04/2017).

[88] N. Perlroth and D. Sanger, *Hacks raise fear over n.s.a.'s hold on cyberweapons*, https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html, Accessed: 28 June 2017.

[89] J. H. Reiman, 'Privacy, intimacy, and personhood', *Philosophy & Public Affairs*, pp. 26–44, 1976.

[90] K. Richardson, 'Sex robot matters – slavery, the prostituted, and the rights of machines', *IEEE Technology & Society magazine*, pp. 46–53, Jun. 2016.

[91] A. Rose, *Are face-detection cameras racist?*, 2010. [Online]. Available: http://content.time.com/time/business/article/0,8599,1954643,00.html (visited on 25/04/2017).

[92] G. Rowe and L. J. Frewer, 'Public participation methods: a framework for evaluation', *Science, technology, & human values*, vol. 25, no. 1, pp. 3–29, 2000.

[93] M. Sax, 'Finders keepers, losers weepers', *Ethics and Information Technology*, vol. 18, pp. 25–31, 2016.

[94] B. Schneier, *A 'key' for encryption, even for good reasons, weakens security*, https://www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security, Accessed: 20 June 2017.

[95] J. Schor, 'Debating the sharing economy', *Journal of Self-Governance and Management Economics*, vol. 4, no. 3, pp. 7–22, 2016.

[96] H. Scott, 'Liability for the mass publication of private information in South African law: nm v smith (freedom of expression institute as amicus curiae)', *Stellenbosch Law Review= Stellenbosch Regstydskrif*, vol. 18, no. 3, pp. 387–404, 2007.

[97] A. Selyukh, *A year after san bernardino and apple-fbi, where are we on encryption?*, `http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption`, Accessed: 20 June 2017.

[98] R. Shafer-Landau, *Ethical Theory: An Anthology*. Wiley-Blackwell, 2007.

[99] S. Simon, L. Howe and H. Kirschenbaum, *Values clarification: A practical handbook of strategies for teachers and students*. A & W Visual Library, 1978.

[100] T. W. Simpson and V. C. Müller, 'Just war and robot's killings', *The Philosophical Quarterly*, vol. 66, no. 263, pp. 302–322, 2016.

[101] D. Smith, *'racism' of early colour photography explored in art exhibition*, 2013. [Online]. Available: `https://www.theguardian.com/artanddesign/2013/jan/25/racism-colour-photography-exhibition` (visited on 25/04/2017).

[102] E. A. nad Sohan Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J.-F. Bonnefon and I. Rahwan, 'The moral machine experiment', *Nature*, vol. 563, pp. 59–64, 2018.

[103] South Africa Constitutional Assembly, *The Constitution of the Republic of South Africa, 1996: as adopted on 8 May 1996 and amended on 11 October 1996*, English. [Constitutional Assembly], 1996, ISBN: 978-0-621-39063-6. [Online]. Available: `http://www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf`.

[104] Statistics South Africa, 'Mid-year population estimates', Statistics South Africa, Tech. Rep. P0302, 2016. [Online]. Available: `https://www.statssa.gov.za/publications/P0302/P03022016.pdf`.

[105] D. A. Strauss, 'Persuasion, autonomy, and freedom of expression', *Columbia Law Review*, vol. 91, no. 2, pp. 334–371, 1991.

[106] Supreme Court of Appeal of South Africa, *History and background*, `http://www.justice.gov.za/sca/historysca.htm`, Accessed: 20 June 2017.

[107] M. Talbot, *Critical reasoning for beginners*, `https://podcasts.ox.ac.uk/series/critical-reasoning-beginners`, Accessed: 17-08-04, 2010.

[108] H. T. Tavani, *Ethics and technology: Controversies, questions, and strategies for ethical computing*, 4th. John Wiley & Sons, 2012, A 5th edition is now avialable. All page numbers refer to the fourth edition. The UCT library has a copy of the 1st edition: 174.9004 TAVA, ISBN: 978-1118281727.

[109] G. Templeton. (Jan. 2016). Free basics, net neutrality, and the problem with charity, ExtremeTech, [Online]. Available: `http://www.extremetech.com/extreme/220106-free-basics-net-neutrality-and-the-problem-with-charity`.

[110] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically aligned design: a vision for prioritizing human well-being with autonomous and intelligent systems', IEEE, Technical report Version 2, 2017. [Online]. Available: `http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html`.

[111] J. J. Thomson, 'The right to privacy', *Philosophy & Public Affairs*, pp. 295–314, 1975.

[112] C. Tredger, *Mobile communication blocked in sa parliament*, http://www.itwebafrica.com/ict-and-governance/267-south-africa/234161-mobile-communication-blocked-in-sa-parliament, Accessed: 17-08-04, Feb. 2015.

[113] A. B. Tucker, 'Computing curricula 1991: a summary of the ACM/IEEE-CS joint curriculum task force report', *Commun. ACM*, vol. 34, no. 6, pp. 68–84, Jun. 1991, ISSN: 0001-0782.

[114] UNESCO, 'Human rights: comments and interpretations', United Nations Educational Scientific and Cultural Organization, Tech. Rep. UNESCO/PHS/3 (rev.) Jul. 1948, p. 276. [Online]. Available: http://unesdoc.unesco.org/images/0015/001550/155042eb.pdf (visited on 14/08/2017).

[115] N. Vallina-Rodriguez, S. Sundaresan, A. Razaghpanah, R. Nithyanand, M. Allman, C. Kreibich and P. Gill, 'Tracking the trackers: towards understanding the mobile advertising and tracking ecosystem', Tech. Rep. 1609.07190, 26th Oct. 2016. [Online]. Available: https://arxiv.org/pdf/1609.07190.pdf.

[116] J. A. Van Dijk, *The deepening divide: Inequality in the information society*. Sage Publications, 2005.

[117] J. Vermeulen, *Alleged cellphone signal jamming at zuma speech*, https://mybroadband.co.za/news/cellular/118821-alleged-cellphone-signal-jamming-at-zuma-speech.html, Accessed: 17-08-04, Feb. 2015.

[118] ——, *Beware bad stats about South Africa*, https://mybroadband.co.za/news/broadband/117502-beware-bad-stats-about-south-africa.html, Accessed: 2017-08-03, Mar. 2015.

[119] D. Vincent, *China used prisoners in lucrative Internet gaming work*, 2011. [Online]. Available: https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam (visited on 25/04/2017).

[120] C. Wainryb, 'Understanding differences in moral judgments: the role of informational assumptions', *Child development*, vol. 62, no. 4, pp. 840–851, 1991.

[121] D. F. Wallace, *This is water: Some thoughts, delivered on a significant occasion, about living a compassionate life*. Hachette UK, 2009.

[122] W. Wallach, 'Toward a ban on lethal autonomous weapons: surmounting the obstacles', *Communications of the ACM*, vol. 60, no. 5, pp. 28–34, 2017.

[123] D. Walton, 'The witch hunt as a structure of argumentation', *Argumentation*, vol. 10, no. 3, pp. 389–407, 1996. (visited on 07/08/2017).

[124] M. Walton, G. Marsden, S. Haßsreiter and S. Allen, 'Degrees of sharing: proximate media sharing and messaging by young people in Khayelitsha', in *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services*, ACM, 2012, pp. 403–412.

[125] M. C. Ware and M. F. Stuck, 'Sex-role messages vis-à-vis microcomputer use: a look at the pictures', *Sex Roles*, vol. 13, no. 3, pp. 205–214, 1985.

[126] M. Warschauer, *Technology and social inclusion: Rethinking the digital divide*. MIT press, 2004.

[127] S. B. Weeks, 'Involving citizens in making public policy.', *Journal of Extension*, 1970.

[128] A. H. Weis, 'Commercialization of the internet', *Internet Research*, vol. 20, no. 4, pp. 420–435, 2010.

[129] Wikipedia, *Websites blocked in mainland china*, https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China, Accessed: 2017-08-03, Aug. 2017.

[130] M. Zapotosky, *Fbi has accessed san bernardino shooter's phone without apple's help*, https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html, Accessed: 20 June 2017.

[131] A. Zwitter, 'Big data ethics', *Big Data & Society*, vol. 1, no. 2, pp. 1–6, 2014.

Appendix A

Glossary

Version 2.3
December 2019

This is an updated version of v2.1 of the glossary of terms on social issues and professional practice for IT and computing. The main changes are: more terms have been added, and they are still split into SIPP terms and purely computer science terms that are relevant within the scope of the SIPP block (that you may not have yet come across in your first year of studies).

The descriptions of the terms are written, for the most part, informally. Longer descriptions can be found in the background reading materials.

Accountability (algorithmic) Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results. (from: ACM statement)

Anonymised data Data that is not directly linked to a particular person. There are different levels of anonymisation, where the level indicates how easy or hard it is to reconstruct to which person the anonymised data belong.

Argument (in informal logic): a form of reasoning that comprises various claims or statements, one of which is being asserted (stated as fact). A valid argument is one where the *Conclusion* follows from the *Premise*s. It can be a useful tool to resolve disputes regarding *Computer ethics* issues and to figure out your own point of view when there is a *Policy vacuum*.

Auditability (algorithmic) Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected. (from: ACM statement)

Autonomous Weapons System A system (hardware+software) that makes decisions autonomously (i.e., without human intervention) for defence or offence purposes, causing physical harm. Also known as Lethal Autonomous Weapons Systems (LAWS) and killer robots.

Big Brother The fictional character in George Orwell's book "1984" that is the leader of a totalitarian state and actually observes everyone constantly. It is now a concept representing abuse of power in the sphere of civil liberties and mass surveillance, be this by the government or other organisations, which is greatly facilitated by ICT.

Code of Conduct A set of rules for good behaviour or proper practices according to the social norms, which the group of people who undersign it should adhere to. For instance, the code of conduct of the Institute of IT Professionals South Africa (IITPSA).

Code of Ethics Similar to *Code of Conduct*, but then more general than just those rules included in a code of conduct.

Computer ethics A branch of applied philosophy that looks at how computing professionals should make decisions about processes (e.g., the programming) or products (e.g., an app, the device).

Conclusion is that statement in an argument that is said to be true and follows from the *Premise*s.

Creative commons A way to legally share on the Web one's intellectual property and copyright on creative works.

Critical reasoning is a branch of informal logic with which one can assess and analyse the arguments that occur in 'every day' natural language discourse.

Deductive argument If the premises are true, then the truth of the conclusion is guaranteed (thanks to the rules of inference). See also *Argument*.

Descriptive statement describes something as a fact (e.g., "the sky is blue"). Generally, they can be tested objectively to verify them. Compare with *Normative statement*.

Digital colonialism refers to the practice that organisations (mainly tech companies) collect and process data from users residing in the Global South for the purpose of exploitation and profit. They then offer services for payment—informed by the data given for free—and push for infrastructural domination while the profits go to those foreign tech companies rather than local ones.

Digital convergence is the trend toward using one device for a range of multimedia uses that used to have separate devices; e.g., watching streaming tv on a computer rather than a TV set, sending emails with your phone rather than from a desktop computer.

Digital divide denotes the gap/difference between people who do have [easy, cheap, fast] access to the internet with all the information on the Web, and those who do not. Strongly related, and often assumed implicitly, are socioeconomic issues that underly the digital divide.

Digital footprint The 'breadcrumbs' trace of data that companies of websites store about your online behaviour, such as which sites you visited, for how long, what you did on their site, and so on.

Echo chamber effect in the context of the Web and social media, it refers to the situation where a user only or mostly sees beliefs or opinions that agree with their own, rather than be exposed to diverse views, which has as effect that their ideas are reinforced.

Ethics is a set of *morally permissible* standards of a *group* that each member of the group (at his/her rational best) wants every other member to follow even if their doing so would mean that he/she must do the same. (Definition copied from Michael Davis' "Profession, Code, and Ethics", p40).

Fallacy indicates faulty reasoning. There are many such 'traps'; e.g. the fallacy of appeal to authority, and an *ad hominem* attack (discrediting the person rather than the argument).

Filter bubble What you see in the search results of a search engine (or feeds in social media) is determined by your prior interaction, rather than a non-personalised page (or item) rank.

Free software is software that is free, with 'free' in the sense of liberty, not price. This means one has the freedom not just to run the software, but also copy, distribute, study, change and improve it. Free software is open source, but open source software is not necessarily also free.

Inductive argument the truth of the premises makes the conclusion more probably true. See also *Argument*.

Information and Communication Technology for Development (ICT4D) seeks to bridge, or narrow the gap of, the *Digital divide*. The term is used mostly in the context of ICT projects in Africa and some countries in Asia and Latin America, and with the aim to develop (broadly construed).

Information and Communication Technology for Peace (ICT4Peace) aims to support peace keeping and peace building efforts for post-conflict and post-disaster reconstruction toward positive peace.

Intellectual property refers to a range of rights of ownership of an (intangible) asset such as a software program, the idea behind it, or some functionality of it. For software, there are four types relevant: patents, copyrights, trade secrets, and trademarks. Its objectives are to promote progress, a fair exchange for mutual benefit for its creator(s) and society, and to create an incentive for inventors and authors to create and disclose their work.

Killer robots Catchy term for *Autonomous Weapons Systems*.

Laws of robotics Science fiction writer Isaac Asimov devised three laws with as aim to regulate what robots are allowed to do, being: 1) A robot may not injure a human being or, through inaction, allow a human being to come to harm; 2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law; 3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Moral agency Moral agency is determined by meeting several conditions, typically: *i)* whether the ethically relevant result is an outcome of the agent's actions (i.e., causality); *ii)* whether the agent had or should have had knowledge of the consequences of its actions; and *iii)* whether the agent could choose another option (generally considered as to be without greater harm for the agent). When at least one of the three conditions is absent, one is, generally, not held morally responsible for the act.

Moral responsibility See also *Moral agency*.

Moral theory is a way of defining *Morality* and provides guidance to answer the two principal questions of how one knows X is good, and why it is good. For instance, one can base it on cultural relativism or religion or that the consequence matter most (instead of the motivation behind it).

Morality is the set of standards everyone (every rational person at his/her rational best) wants everyone else to follow even if their following them means having to do the same. (Definition copied from Michael Davis' "Profession, Code, and Ethics", p41).

Net neutrality is the principle that all data packets sent over the Internet are treated equally.

Normative statement explores what people ought to do. They are prescriptive and they try to provide an account of why certain behaviours are good/bad or right/wrong. Compare with *Descriptive statement*.

Open Source Software Software of which the source code is publicly available. Its copyright holder provides people the rights to study, modify, and (re)distribute the code to anyone.

Panopticon Institutional building design by English philosopher Jeremy Bentham (late 18th century) that aimed that one watchman would, all at once, be able to observe all inmates of the prison. This is physically impossible, but the real issue is that the inmates will not know when exactly they are being watched, resulting in that all inmates must self-control their behaviour as if they are being watched. See also *Big Brother*.

Policy vacuum The speed of innovations outpaces the slowness of devising policies and laws how to deal with the new technologies, leaving a 'vacuum' where events and practices occur. These events and practices, while unintentionally not illegal, may still be unethical or immoral.

Premise a statement that is being offered as a reason for believing the truth of the *Conclusion* of an *Argument*.

Privacy The person's [right to/ability to/state of] being secluded from other people, having control over information about oneself.

Problem of 'many hands' refers to the situation where multiple actors are involved in the development and deployment of technologies, which makes it hard to identify who exactly did what. This negatively affects the process of assigning blame when a technological accident occurs, as well as who to praise for its success.

Provenance of data, information, and knowledge has a 'trail' (description) where it originates from, including the original source(s), how it was collected, cleaned, and processed.

This now also is expected to be accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process (from: ACM statement).

Surveillance capitalism refers to a business model where "profits derive from the unilateral surveillance and modification of human behavior" made possible by the advances in IT hardware and software, as formulated by Zuboff (2016).

Trustworthy software is defined as the enhancement of the overall software and systems culture, with the objective that software should be designed, implemented and maintained in a trustworthy manner. (e.g., the British Standards Institution PAS 754 Software trustworthiness).

Ubuntu Roughly translates to humanness, humanity (and also interpreted as "I am, because we are; and since we are, therefore I am"). It is also the name of a free and open source operating system.

Ubuntu morality is described (by T Metz) as that an action is right just insofar as it promotes shared identity among people grounded on good-will; an act is wrong to the extent that it fails to do so and tends to encourage the opposites of division and ill-will.

Relevant computing terms

Artificial Intelligence A branch in computer science and IT that concerns the theory and development of computer systems that can carry out tasks that normally requires human intelligence, i.e., to simulate 'intelligent' behaviour in computers. This include subfields that focus on techniques for learning and reasoning using, among others, logic, statistics, language.

Big Data It has no single definition, but there are either 3 Vs or 5 Vs associated with it: Volume, Velocity, and Variety, to which Veracity, and Value have been added more recently. That is, respectively: the huge amounts of data, the speed at which they are generated, the different types of formats of the data, the trustworthiness of that data, and the money one can make with it.

Cloud computing refers to services hosted on large data centres (including 'server farms') offered over the Internet. Such as collection of devices are presented to the user as if it is one entity that is used for data storage and computation by software applications that are run remotely.

Conceptual data model An implementation-independent model of the data that has to be stored and processed within the application domain; e.g., a UML Class Diagram.

Data analytics processing and analysing large amounts of data starting from some hypothesis, and its results are typically used for decision-making. See also *Data mining* and *Machine learning*.

Data mining refers to the process of exploration and analysis of large amounts of data by automatic or semi-automatic means so as to discover meaningful patterns and rules. See also *Data analytics* and *Machine learning*.

Database is a structured collection of data such that it facilitates easy manipulation and retrieval of that data by a database management system (the software processing the text file), such as the *Open source software* PostgreSQL.

Internet of Things adds to the common Internet the connectivity of devices that are not regarded as computers but that do have embedded electronics so that they can be interacted with remotely, including, e.g., sensors, fridges, smart home appliances like a security system.

Linked Data Structured data on the Web that can be linked across different sources, i.s., facilitate information integration, and be queried as one big graph. See also *Semantic Web*.

Localisation This refers mostly to localisation of software, meaning, at least, the translation of terms used in an application's interface into the language spoken where that software is used, and other features, such as spelling and grammar checking for one's language and autocomplete for words in one's language. Hardware localisation manifests itself practically for endusers as different keyboard layouts.

Machine Learning focuses on algorithms to achieve good predictions based on large amounts of training data. See also *Data mining* and *Data analytics*.

Reasoning, automated a way to infer implicit knowledge from explicitly represented information, using the rules of inference together with a logic in which the information is represented and a set of algorithms that automate this process.

Web 2.0 The Web with m:n information flow between entities, such as blogs with comments, forums integrated in webpages, social media sites to share information with friends. This contrasts with the 'first generation' Web that was just 1:n information flow between an information provider and many consumers.

Web 3.0 See: *Semantic Web*.

Semantic Web The Web with meaning added to it (cf. plain text in HTML files and just keywords), where the meaning is represented formally and one can make inferences automatically. *Linked Data* is a component of the Semantic Web.

Appendix B

Changelog

These lecture notes are a work in progress. Every 5-7 years, there is a major update to reflect the main changes in the field. Major updates take time, however, so it is generally distributed among several academics within the department who update bits and pieces to get the most outdated material out of the way and updated with the changing landscape of current ethical issues in IT & computing, yet not become overly overworked or have too much detrimental effect on research. This version you have in front of you now, is the culmination of one of those major updates.

The major updates in this case were driven by 1) topic updates, as new issues have come to the fore (e.g., Big Data, the 4th industrial revolution, autonomous vehicles), 2) curriculum changes driven by, among others, the ACM, the BCS, and the higher education climate in South Africa, which acknowledge better that SIPP is a core component of the computer science curriculum, and 3) a harmonisation of two modules at UCT, being the conversion Masters in IT's SIPP course CSC5014Z and the 1st-year computer science course's SIPP section of CSC1016S, where some students enrolled in the latter had come across lecture notes for the former, and wanted something similar. The course descriptions and requirements are not exactly the same, so a lowest common denominator is used for these notes, nor is the profile of the students the same. For instance, some more advanced reading of scientific literature is required for the M.IT SIPP module and they may have come across issues in the field during their work already, whereas for CSC1016S there are also slides, class content and discussions, and pop quiz questions that introduce the various topics. All your course material is examinable.

An attempt at listing updates is made in the table below. If you have any feedback on the material, you're welcome to contact the lecturer of your SIPP module.

Maria Keet
Cape Town, December 2019

Table B.1: Main changes throughout the decades.

Version	When	Author	Main updates
v4	2019	Maria Keet	Ch1 minor edits; Ch2 major edits and additions (including new §2.1.2, §2.3.x, §2.6); minor edits to Ch3-4, old ch8 as §4.6; new §5.3; updates to Ch6, §6.1.3, §6.2; more references; added glossary, changelog
v3.5	2018	Melissa Densmore	new §5.1.4 and §6.4, extended §6.1
v3	2017	Edwin Blake	Major revisions to ch1-4; added bibliography; presentation and layout
v2	2009?	?	Dated text indicates there have been updates around that time
v1	Around 2000s	Middlesex University, UK	This is were the first notes originate from, thanks to a agreement made between Middlesex University and UCT