

Ethical, Legal and Social Aspects of Systems

Siri Fagernes, Kirsten Ribu

University College Oslo, Faculty of Engineering, Norway

E-mails: siri.fagernes@iu.hio.no, kirsten.ribu@iu.hio.no

1. Introduction

Communication networks have altered many aspects of life, like work and employment, healthcare, transportation and entertainment. Technology has brought many benefits, but is also the cause of many social and ethical concerns: system failures, the destruction of property, the so-called *digital divide*, workplace monitoring, Internet censorship, and the increasing gap between rich and poor, are some examples of important ethical questions that arise when we reflect on how technology has impacted modern life.

System Administrators play an important part in keeping networks secure. They are also responsible for the uninterrupted operation of the computers to take care of the business needs. A system administrator's duties and responsibilities encompass more than technical knowledge. They are given broad access to the resources of computer systems because their job responsibilities require such access. For instance, in troubleshooting email issues, a system administrator may have to go through the employees' email, but must treat any knowledge so gained as private. Many companies have codes of ethics for employees who in the nature of their job have privileged access to company systems. The content of such codes may include statements like: "do not browse through the computer information of system users while using the powers of privileged access unless such browsing: is a specific part of the job description, do not disclose computer information observed while operating with privileged access, do not copy any computer information for any purpose other than those authorized under their defined job responsibilities, report suspicious incidents to management or police" and so on. Such codes of ethics provide guidelines for

1 professional conduct, and are useful tools. However, situations do arise where it may be
 2 hard to decide what to do, for instance, how would you react if your boss asks you to go
 3 through all the employees' email?
 4
 5

6 **2. Social aspects of technology**
 7

8 New technologies have blossomed during the past century, and have had a tremendous
 9 impact on our way of living. Automated methods for developing all kinds of products
 10 have lowered the costs and hence the prices, which again has lead to increased purchasing
 11 power for households. Less manual labor has reduced the physical strain on the human
 12 body, which combined with improved methods within the medical profession, has lead to
 13 increased life expectancy.
 14

15 However, the overall effects of new technology are never fully predictable, and it is
 16 obvious that there are several side effects to this development. While less manual labor has
 17 led to less physical strain, various health problems might emerge through inactivity. While
 18 technology has lead to automated production and increased productivity, the people who
 19 earlier performed this work manually have become obsolete.
 20

21 These and other important issues call for increased awareness regarding introduction of
 22 new technology, concerning both short-term and long-term effects on our society. In this
 23 section we will present several areas that should be studied in more detail.
 24
 25

26 **2.1. Health issues**
 27

28 When discussing the social implications of technology, the ones perhaps raising the biggest
 29 concerns are those connected to human health. Increased access to technology has reduced
 30 the need for human physical labor, and hence reduced the severe physical strain on the
 31 human body as a result of daily work. Also, the expected age has increased dramatically
 32 as a result of progress within the medical sciences, assisted by better technologies to aid
 33 laboratory analysis, test-taking, speeding up the process for giving diagnosis to illnesses
 34 and so on.
 35

36 However, the dramatic increase in the use of so-called *ICTs* the last decade, has also
 37 meant increased exposure to other negative side-effects. Extensive research has been per-
 38 formed on this issue, but it seems very difficult to come to any clear conclusion.
 39

40 When discussing the health effects of information and communication technology, one
 41 distinguish between the physical effects and the psychological effects. It might be of no
 42 surprise that the physical effects of ICT on the human body are a lot simpler to investigate
 43 than the psychological effects. The first are also the best documented of the two [3]. Of the
 44 physical side-effects, the following are among the most common:
 45

1. *Weight issues.* The extensive use of ICTs, at home, in schools and at work, has lead
 to less physical activity, and hence to an increase in the number of cases of serious
 overweight or obesity.
2. *Repetitive strain injuries.* As a result of extensive use of a computer mouse or joy-
 stick, severe pain in arms and shoulders has been a common problem for those using

a computer as a daily routine. Also, spending long hours sitting in front of a computer screen often lead to extensive strain on the upper body including the back region.

3. *Vision.* The development of the eyes/vision of children could have negative effects of the radiation from TVs and CRT-screens.

4. *Artificial light.* Some types of artificial light (television screens and computer CRTs) might be harmful to biological organisms.

5. *Radiation.* Our daily exposure to electromagnetic signals from several types of networked devices might pose potential risks.

On the psychological side, the results are a bit more difficult to interpret, since the *content* of the media studied could be as important as the amount of consumption [3]. However, there are suggestions of certain physiological effects. Research has shown clear correlations between heavy use of media (television, Internet, video games etc.) and signs of depression and anxiety among young people [3]. Information overload, and the fact that youngsters are not mentally prepared for all these impressions are listed as causes.¹

Other aspects that could be affected are the general intellectual development, attention span and imagination of users. One particular example is the reliance of external stimulation as a result of heavy consumption of ICT-related media. Also, addiction to certain activities as a result of the new technologies might be a problem in the near future.

2.2. Employment and work

A common perception is that innovations in technology result in fewer available jobs, because automated production makes human labor redundant. Investigations show that several branches have suffered from reduction in the number of available jobs, both within manufacturing and so-called ‘white-collar’ jobs [19].

On the other hand, there exist several examples of how innovations within technology have lead to an increase in the number of available jobs, because new technology creates a need for new job functions. Also, innovations cause prices of different goods to drop, again leading to increased purchasing power among people in general, which again leads to increased demand for the products, and hence more jobs.

Teleworking, as a result of improved communication technology, has resulted in improved working conditions for those dependent on working from home. This makes it possible for single parents without means to pay for child care, people living in rural areas, and others who normally would have difficulties working normal office hours, to take part in the job market. However, common experiences are a lack of contact with colleagues and office environment, difficulties in separating office hours and leisure time, since office and home are at the same location, and sometimes missed opportunities in getting promoted.

2.3. Changing social and group-dynamical patterns

One of the most influential technological changes during the last decade has been the mobile phone. Teenagers have adopted this new technology and let it change the way they

¹Editorial comment: Omega-3 deficiency has been related to youth apathy and media addiction in trials in the U.K. indicating that media dependency is part of a wider problem.

1 interact and keep in touch, even using it as a basis for organizing their circle of friends. 1
 2 This is an example of how *not* having a cellular phone could cause one to be excluded 2
 3 from the social community, as it is the main source of communication and exchange of 3
 4 information. 4

5 In the Internet community, there are examples of office environments changing their 5
 6 meeting habits, now using chatrooms as a forum for office meetings. When meetings and 6
 7 general discussions take place ‘online’ instead of in a physical meeting room, changes in 7
 8 group dynamics emerge, such as who dominates the group, as there typically are different 8
 9 skills needed to succeed online. This is an example of how new technology might funda- 9
 10 mentally change the way humans interact, and affect which groups that benefit from the 10
 11 interaction form. While typical ‘nerds’ might be intimidated by physical meetings, they 11
 12 can ‘rule’ online. 12

13 New technologies also have an impact on the family and home environment. Teenagers 13
 14 tend to adopt new technology more easily than their parents, and hence gain more ‘power’ 14
 15 in the home, as they become the ‘gurus’ of the family. This has several implications for the 15
 16 dynamics between parents and their children. For instance, how can the parents control 16
 17 the Internet user habits of their children if the children are in charge of the computers in 17
 18 the home. This phenomenon disturbs the normal family pattern where the parents are the 18
 19 role models. 19
 20
 21
 22

23 **2.4. The digital divide** 23 24

25 As information technology has gained foothold in our society, a phenomenon known as the 25
 26 *digital divide* has emerged. A common definition of the digital divide is *the situation where* 26
 27 *some people have access to modern information technology while others do not.* [19]. Usua- 27
 28 lly one speaks of the *global* and the *social* divide, where the global divide is a measure 28
 29 of the difference in Internet access between developed and less developed countries, while 29
 30 the social divide is a reference to the difference between individuals within the same coun- 30
 31 try [19]. Parameters affecting the level of Internet access within a particular country are, 31
 32 among others, race, income level and age group. 32

33 The global divide is illustrated by the numbers of people in the world with Internet 33
 34 access. In June 2006, approximately 1,043 million people worldwide use the Internet, ac- 34
 35 cording to Internet World Stats. The United States, Australia and Europe are well above 35
 36 the average, while other parts of the world are below. In Africa, only about 1 out of 200 36
 37 persons had Internet access in 2000 (2.6 percent). Because of the high numbers of Internet 37
 38 users in the West, one tends to forget that most people in the world actually have little ac- 38
 39 cess to not only the Internet, but also telephones, health care, education and books. These 39
 40 problems are caused by poverty, isolation and politics. Also, there is a digital divide in the 40
 41 United States and other western countries between the rich and the poor, people of different 41
 42 age groups, and between people of different ethnical background. The consequences are 42
 43 serious: people who have not acquired basic computer skills will have trouble finding jobs, 43
 44 and will have little chance to escape poverty. Thus, the global digital divide will continue 44
 45 to exist. 45

1 When discussing the digital divide, one important concept is *technological diffusion*, 1
2 which refers to *the rate at which a new technology is assimilated into a society*. There exist 2
3 two common theories on how this happens: 3

4 1. *The normalization model*. This model predicts that *everyone* in a society will eventu- 4
5 ally adopt to a new technology, but that the wealthiest part of the population adopts 5
6 first, then the middle range, and finally the least wealthy part. This model is referred 6
7 to as the ‘optimistic’ model. 7

8 2. *The stratification model*. This model predicts that the income groups will adopt in 8
9 the same order as the other model, but it contradicts in the sense that it claims that 9
10 a larger percentage of the wealthier groups will adopt than the less wealthier. This 10
11 means that a certain part of the population will *never* take to the new technology, and 11
12 describes a pessimistic model. 12

13 The reason why the digital divide is such a concern nowadays, is the relationship be- 13
14 tween ‘digital literacy’ and general wealth or success. Some of the criticism against the 14
15 digital divide lies in the fact that it appears that digital literacy follows from general suc- 15
16 cess, and not the other way round. 16

17 3. Ethics 17

18 3.1. Ethics and morality 18

19 The term ‘ethics’ defines the philosophical study of morality, whereas the term ‘morality’ 19
20 refers to the way we live and act. To simplify this, we can say that if the traffic laws 20
21 and regulations are the underlying ethics of driving, morality is abiding by these laws and 21
22 regulations. Speeding and drunk driving is obviously immoral conduct. Some behavior 22
23 is not regulated by law, but rather agreed on, for instance polite and considerate driving. 23
24 Traffic bullies are therefore immoral. In this way we see that ethics reach beyond the law, 24
25 and philosophers have at all times occupied themselves a great deal with the theoretical 25
26 study of ethics, or moral philosophy. There are many different perspectives on ethics, as 26
27 we shall see. 27

28 Ethical dilemmas arise when we are faced with problems of right or wrong. The differ- 28
29 ence between right and wrong may be hard to determine, and is not necessarily a question 29
30 of what is legal. Tying ‘good’ and ‘bad’ to expressions of approval or disapproval of human 30
31 actions may be difficult, because things can be good or bad independently of our personal 31
32 approval or disapproval of them [22]. 32

33 Certain ethical judgments can be classified as feelings or emotions, and these are nei- 33
34 ther true or false. This view is known as emotivism. However, most philosophers refer to 34
35 our actions and intentions when discussing moral matters, not to our emotions, because 35
36 this belongs more to the field of Psychology. The challenge of showing that people are 36
37 better off acting morally than immorally may be difficult. Personal gain and individual 37
38 convictions play an important part in most peoples lives. Although we know that copying 38
39 proprietary software or downloading music may be illegal, many people are opposed to the 39
40 laws regulating such activities, and defend their actions by attacking unpopular regulations. 40
41 So in order to decide whether something is good or bad, right or wrong, one must rely on 41
42 42
43 43
44 44
45 45

1 experience and common sense, and judge by the consequences or intentions of the act. 1
 2 A knowledge of ethical principles may be a help when trying to analyze difficult ethical 2
 3 dilemmas. 3

4 Changes in technology require changes in laws and personal attitudes. The use of com- 4
 5 puters can cause new ethical dilemmas because people are pushed into unforeseen situa- 5
 6 tions. Although many questions that arise from the use of computers are not very different 6
 7 from problems encountered in other aspects of life, the activities on the Internet, the sheer 7
 8 size of the World Wide Web and the amount of available information often create new 8
 9 ethical dilemmas. Computers are a part of our everyday life, both professional and private, 9
 10 and we are dependent on computer networks in all parts of society. A problem with a com- 10
 11 puter system may negatively impact a whole company, the company's business partners, 11
 12 financial interests as well as hundreds of users. The interest in ethical reflection on the use 12
 13 of computer systems is steadily growing, and the study of ethics is incorporated into the 13
 14 computer science curricula in many universities and colleges. 14

15 The growth of the Internet has created several new legal issues. Boundaries are no longer 15
 16 geographical, and this fact can be used to circumvent national laws. For instance, Internet- 16
 17 based casinos are illegal in many countries, therefore, gambling web-sites are run from 17
 18 places like the Caribbean or Malta. Some of the main concerns in computer ethics today are 18
 19 questions of copyright, privacy and censorship. Traditional rules of conduct are not always 19
 20 applicable to a new medium. It is necessary to reflect on questions like the following: If a 20
 21 certain nation wishes to protect freedom of speech on the Internet, whose laws apply? What 21
 22 about censorship on the Internet? A national constitution protecting freedom of speech is in 22
 23 a sense a local law which does not necessarily apply in other countries. How can issues like 23
 24 freedom of speech, protection of intellectual property, invasions of privacy be governed by 24
 25 law when the whole world is involved? 25

26 It is important to become aware of the fact that there are not necessarily correct answers 26
 27 to ethical dilemmas. Every computer professional should therefore have some knowledge 27
 28 of international law and best practices, and an awareness of the responsibilities tied to the 28
 29 job, and be acquainted with the codes of ethics that exist for members of the profession. He 29
 30 or she should reflect on how to deal with ethical dilemmas in situations where there may 30
 31 be considerable pressure to do something illegal or ethically wrong. 31

32
 33
 34 **3.2. What are computer ethics?** 34
 35

36 Ethics and values are today discussed in a context that is not limited to a particular geo- 36
 37 graphic region, a specific religion or culture. Much of the discussion on ethics today has to 37
 38 do with the use of modern technology. Computers are everywhere, playing a large part of 38
 39 peoples' lives, both professionally and in the filed of entertainment end relaxation. Com- 39
 40 puter ethics can therefore be understood as that branch of applied ethics which studies and 40
 41 analyzes social and ethical impacts of information technology. 41

42 Computer ethics involve the use of computers, networks and the Internet, and therefore 42
 43 also include global information ethics. Computers have become commonplace, and have 43
 44 great impact on society and the transformation of culture. Because computers have become 44
 45 universal and are part of our daily lives, many ethical problems have to do with computer 45

1 ethics. Although problems involving computing connect with every-day ethical issues in 1
2 some way, the field of computer ethics is also unique because of the technology itself. 2
3 Computers can be designed to perform any task we wish. They are universal tools that 3
4 can be used in so many ways that it is difficult to foresee all the situations that may arise. 4
5 Therefore, we do not always have traditions or policies to act as ethical guidelines. 5

6 Computers tend to create more novel situations and dilemmas than other tool and tech- 6
7 nologies. The technology provides opportunities for misuse. For instance, newspapers 7
8 commonly report stories about identity theft on the Internet, body parts being sold, viola- 8
9 tion of copyright and privacy, illegal monitoring, terrorists and criminals using the Internet 9
10 for their own ends, and crimes like the spreading of child pornography. 10

11 A great deal of literature on computer ethics discusses the laws and regulations concern- 11
12 ing such issues and the use and misuse of the Internet, freedom of speech, privacy, intel- 12
13 lectual property, and professional conduct. However, ethics reach beyond the law. Modern 13
14 technology is developing at a tremendous speed, and traditional ethical theory and every 14
15 day morals do not always help us to make the right decisions when dealing with computer 15
16 technology. A system administrator comes into contact with privileged information and 16
17 must protect the confidentiality of all such information. However, a system administrator 17
18 may be pressured into exposing such information, for instance snooping in employees' 18
19 e-mail. The knowledge of ethical principles may serve as a help in order to decide how to 19
20 act morally under pressure. 20

23 3.3. Ethical principles 23

25 Moral truths are those truths that are accepted by many people, despite differences in 25
26 culture and religion. One example is Human rights. Others could be deeds that create peace 26
27 and harmony between people. Ethical rules like “do not steal or cheat, keep promises, pay 27
28 your debts and do not lie” ensure that we live good lives in interaction with other people. 28
29 So how do we decide what is good, fair and honest, in short, how do we behave ethically? 29
30 One way of looking at it is to place focus on what we ought to do, not what we want to 30
31 do, which means acting in a certain way according to moral rules. For instance, in a pro- 31
32 fessional context, doing good ethically means doing a good job. On the other hand, good 32
33 qualities do not necessarily lead to good deeds. Intelligence and courage are good qualities, 33
34 but can be used in harmful way, for instance for robbing banks, fraud etc. 34

35 A useful ethical theory makes it possible for us to examine moral problems, reach 35
36 conclusions through logical reasoning and defend the conclusions. Philosophers have 36
37 always discussed moral matters. Formal study of ethics goes back to the Greek philosopher 37
38 Socrates. Philosophers have proposed many ethical theories. Traditionally, there are sev- 38
39 eral moral perspectives, for instance ethical principles of consequence (utilitarianism), duty 39
40 and virtue, formulated by the philosophers John Stuart Mill, Immanuel Kant and Aristotle 40
41 respectively. A few words about these moral perspectives will help to understand different 41
42 views on ethics, and show that as individuals, people think differently about moral values. 42
43 One should regard these theories as tools, or as the ‘operating system’ for our behavior as 43
44 human beings. The theories exist as moral perspectives underlying our actions, but are not 44
45 visible in our every-day lives. 45

1 There are three main categories of practical ethical theories, or normative ethics. *Nor-* 1
 2 *mative ethics* is the philosophy of practical moral standards that tell us what is right and 2
 3 what is wrong, and how to live moral lives. They focus on the virtues and good habits that 3
 4 we should acquire, the duties that we should follow, or the consequences of our behavior. 4
 5 These three categories are the ethics duty (deontology), consequence and virtue. 5

6 The *theory of duty* (deontology) focuses on the study of right and wrong, obligation, 6
 7 permissions and duty. Theories of duty propose standards of morality, moral codes and 7
 8 moral rules. One rule that is well known is the so-called golden rule: “Do unto others as 8
 9 you would have them do unto you”. This rule focuses on good deeds. Many companies 9
 10 today have moral codes for company behavior based on this principle. 10

11 Another way of looking at ethics of duty it is to consider what it means to do good by 11
 12 acting according to good will. Good will is the only thing that can be called good without 12
 13 qualification. Is not the same as good deeds, but good in itself. Doing the right thing with 13
 14 no thought of the consequences is an act of duty and good will. 14

15 *Utilitarianism* or the *ethics of consequence* (from the Latin *utilis*, useful) is a theory of 15
 16 ethics based on quantitative maximization of good for society or humanity. This good can 16
 17 be viewed as happiness or pleasure. Utilitarianism is a form of consequentialism, meaning 17
 18 that an act should be judged by the consequences of that act. Utilitarianism is sometimes 18
 19 summarized as “*The greatest happiness for the greatest number of people*”. Sometimes 19
 20 people say: ‘If I had known the consequences, I would not have acted in this way’. Knowing 20
 21 what is good in a consequentialistic perspective may become more clear in hindsight. 21

22 *Virtue ethics* may be identified as the one that emphasizes the virtues, or moral character 22
 23 of a person. In contrast to the approach which emphasizes duties or rules. In philosophy, 23
 24 the phrase *virtue ethics* refers to ethical systems that focus primarily on what sort of person 24
 25 one should try to be. According to virtue ethicists the aim of all humans is to lead a good, 25
 26 happy and fulfilling life. 26

27 An ethical principle is a tool for considering whether an act is morally right or wrong. 27
 28 In order to illustrate the difference in the three perspectives described above, we can say 28
 29 that in the case of rescuing a drowning person, a *utilitarian* will point to the fact that 29
 30 the consequences of jumping into the water and pulling the person out will maximize 30
 31 everybody’s well-being, the rescuer’s own included, since good deeds are rewarded, a *duty* 31
 32 *ethicist* will state that a rescue act is in accordance with the moral rule “*do unto others as* 32
 33 *you would be done by*”, and not think of any personal gain, whereas a *virtue ethicist* simply 33
 34 knows that rescuing the person is a charitable act, and will do so accordingly. 34
 35
 36

37 4. Professional ethics 37

38
 39 Professional ethics differ from general ethics. The professional is an expert in a field that 39
 40 the customer knows little about, for instance computer science or medicine. Customers rely 40
 41 on the knowledge, expertise and honesty of the professional. The products (medicine, com- 41
 42 puter networks, bridges, investment advice) affect large numbers of people. A computer 42
 43 professional’s work can affect the life, health, finances, freedom and future of a client or 43
 44 a group of people. A professional can cause great harm through dishonesty, carelessness 44
 45 or incompetence. People are often unable to protect themselves, not being involved in the 45

1 choice of tool or product. Therefore, computer professionals have responsibilities to the
2 general public.

3 Professional Ethics concern one's conduct of behavior and practice when carrying out
4 professional work. Any code may be considered to be a formalization of experience into
5 a set of rules. A code is adopted by a community because its members accept the rules,
6 including the restrictions that apply. Apart from codes of ethics, professional ethics also
7 concern matters such as professional indemnity. No two codes of ethics are identical. They
8 vary by cultural group, by profession and by discipline.

9 It is often assumed that universal ethical principles exist. However, it is a fact that in
10 some cultures, certain behaviors are unacceptable, but in other cultures the opposite may
11 be true, for instance when it comes to the question of software piracy, several viewpoints
12 exist. Richard Stallman of the Free Software Foundation [5] for instance has argued at
13 length about the superiority of freedom over protectionism in software licensing.

14 In many situations, there are several options that may be ethically acceptable. It is there-
15 fore misleading to divide all acts into two categories: ethically right and ethically wrong.
16 One should rather view acts as ethically obligatory, prohibited or acceptable. One way to
17 try to define these categories are by creating codes of ethics.

18 After episodes like the Enron scandal of 2001, focus is increasingly placed on ethical
19 behavior in business.² The Enron Corporation was an American energy company based in
20 Houston, Texas, United States. Enron employed around 21,000 people and was one of the
21 world's leading electricity, natural gas, pulp and paper, and communications companies.
22 It went bankrupt in 2001, when it was revealed that its reported financial condition was
23 sustained mostly by systematic accounting fraud. It was the biggest bankruptcy in US
24 history, costing 4,000 employees their jobs. The scandal has become a popular symbol of
25 willful corporate fraud and corruption [30].

26 Many large companies today are being pressured into acting morally, and are forced to
27 take ethics seriously as a part of their culture. There is a heightened awareness of ethical
28 issues in many societies. Attitudes change, and hopefully, corporate businesses will place
29 ethics higher than profit. Corruption can then be more easily revealed, and experience will
30 show that good ethics will pay in the long run. One reason is that customers are more likely
31 to trade with a business known to be honest and trustworthy. Also, employees will join and
32 faithfully serve a company that treats its workers with loyalty and respect.

33 Although assuming that doing the right thing pays, it is still not easy to know the best
34 way to balance duties to shareholders, the rights of employees, service to customers and
35 obligations to society. But a good ethical policy can help develop a more honest corporate
36 culture.

37 According to Deloitte and Touche, "*companies that follow both the letter and the spirit*
38 *of the law by taking a 'values-based' approach to ethics and compliance will have a dis-*
39 *tinct advantage in the marketplace". Deloitte has suggested guidelines for writing a code*
40 *of ethics, emphasizing how an organization should develop its own code to suit the needs*
41 *of "its personnel in defining expected behaviors and in addressing the risks, challenges,*
42 *and customs in the countries in which it operates, as well as to fit their specific industry*
43 *and situation" [23]. The code should not be written as a list of 'do not's' but state expected*

44 ²Editorial comment: the Sarbanes–Oxley (SOX) act was introduced as a measure to avoid future debacles in
45 the US.

behavior, and be global in scope. This example demonstrates that serious attempts are being made in the world of business to behave ethically, although there are, unfortunately, numerous examples of the opposite. However, companies risk having their unethical activities exposed by whistleblowers, who are within their rights to do so, and may be protected by whistleblower protection acts.

4.1. *Ethical and professional conduct in system administration*

It is useful to have general guidelines for professional and ethical conduct like the codes of ethics referred to above, but ethical dilemmas arise in unexpected situations, and as a systems administrator you may be at loss what do you do when for instance you are asked by a colleague or your boss to read someone else's e-mail, or you come across information that reveals plans for sabotaging the company, stealing equipment and reselling via online auction, or illegal financial activities in your company. There are numerous such examples, and you may be faced with a choice: Either 'blow the whistle' and risk losing your job, or keep the information to yourself, having to live with the knowledge that you have maybe not acted ethically.

Regrettably, there are no simple answers to these dilemmas. Moral philosophy assumes that people are rational and make free choices since free choice and the use of rational judgment are characteristics of human beings. Ethical principles may help us out in difficult situations. However, it is human to make mistakes. Besides, a person may not be making a free choice when he or she risks losing a job. Difficult dilemmas arise in professional life, for instance, admitting to a customer that your software is faulty, declining a job for which you are not qualified or speaking out when you know something is wrong takes courage, and is not always rewarded.

The role of the system administrator

A system administrator's job is to ensure proper operation, support, and protection of a company's network services and to take all security measures to protect the computers and the data contained on them. System administrators have access to an enormous amount of information, and therefore have great power and responsibility. This responsibility also includes abiding by copyright laws, as companies caught using pirated software have significant legal and financial liabilities. Protecting the integrity of information includes ensuring that unauthorized users access or make changes to data not belonging to them. System administrators are often blamed for copyright violations found on their networks.

Generally, smaller companies employ one or two system administrators to look after the organization. The scenario is different in larger organizations, where there is a larger number of system administrators, each responsible for a specific role within the system.

Unlike many professions, there is no single path to becoming a system administrator. In some cases, candidates are required to possess industry certifications before being considered, but since few colleges or universities have specific programs for system administration, many systems administrators are self-taught. This means that a system administrator

1 may be lacking in knowledge of legal matters and ethical and professional conduct. We 1
2 therefore seek to give an overview of some important topics that may be useful in order to 2
3 become aware of ethical questions and how to solve dilemmas. We present references to 3
4 international laws and regulations, ethical codes and online help-centers. It is our aim to 4
5 enhance reflection and conscious decision-making. 5
6 6
7 7

8 **4.2. Codes of ethics** 8 9 9

10 Codes of ethics are concerned with a range of issues, including academic honesty, adher- 10
11 ence to confidentiality agreements, data privacy, handling of human subjects, impartiality 11
12 in data analysis and professional consulting, professional accountability resolution of con- 12
13 flicts of interest and software piracy. 13

14 Many computer professionals are members of organizations like the ACM or the IEEE, 14
15 and so have agreed to be bound by one of the following: 15

- 16 ● The ACM Code of Ethics and Professional Conduct. 16
- 17 ● The ACM/IEEE Software Engineering Code of Ethics and Professional Practice. 17
- 18 ● The IEEE Code of Ethics. 18

19 These codes are rather general in their phrasing. They present lists of do's and don'ts, 19
20 which are easy to agree with, but do not necessarily help us out when we are faced with 20
21 serious ethical dilemmas. The ACM Code includes general moral imperatives, such as 21
22 “avoid harm to others” and “be honest and trustworthy”. The code also included more 22
23 specific professional responsibilities like “acquire and maintain professional competence” 23
24 and “know and respect existing laws pertaining to professional work” [23]. The IEEE 24
25 Code of Ethics includes such principles as “avoid real or perceived conflicts of interest 25
26 whenever possible” and “be honest and realistic in stating claims or estimates based on 26
27 available data” [24]. 27

28 The Accreditation Board for Engineering Technologies (ABET) has long required an 28
29 ethics component in the computer engineering curriculum. And in 1991, the Computer Sci- 29
30 ences Accreditation Commission/Computer Sciences Accreditation Board (CSAC/CSAB) 30
31 also adopted the requirement that a significant component of computer ethics be included in 31
32 any computer sciences degree granting program that is nationally accredited. Professional 32
33 organizations in computer science recognize and insist upon standards of professional re- 33
34 sponsibility for their members. 34
35 35
36 36

37 *The ACM software engineering code of ethics and professional practice* 37 38 38

39 The Association for Computing Machinery (ACM) has created a code of professional 39
40 ethics for software professionals. “Commitment to ethical professional conduct is ex- 40
41 pected of every member (voting members, associate members, and student members) 41
42 of the Association for Computing Machinery (ACM)”. This Code, found at the URL 42
43 <http://www.acm.org/constitution/code.html>, “consists of 24 imperatives formulated as 43
44 statements of personal responsibility, and identifies the elements of such a commitment. 44
45 It contains many, but not all, issues professionals are likely to face. . . It is understood that 45

1 *some words and phrases in a code of ethics are subject to varying interpretations, and* 1
 2 *that any ethical principle may conflict with other ethical principles in specific situations.* 2
 3 *Questions related to ethical conflicts can best be answered by thoughtful consideration of* 3
 4 *fundamental principles, rather than reliance on detailed regulations” [24].* 4

5 The code says: 5

6 *As an ACM member I will...* 6

- 7 1.1. Contribute to society and human well-being. 7
- 8 1.2. Avoid harm to others. 8
- 9 1.3. Be honest and trustworthy. 9
- 10 1.4. Be fair and take action not to discriminate. 10
- 11 1.5. Honor property rights including copyrights and patents. 11
- 12 1.6. Give proper credit for intellectual property. 12
- 13 1.7. Respect the privacy of others. 13
- 14 1.8. Honor Confidentiality. 14

15
 16 *ACM/IEEE-CS joint task force on software engineering ethics and professional practices* 16
 17 17

18 Software engineers shall commit themselves to making the analysis, specification, design, 18
 19 development, testing and maintenance of software a beneficial and respected profession. In 19
 20 accordance with their commitment to the health, safety and welfare of the public, software 20
 21 engineers shall adhere to the following ‘Eight Principles’: 21

22 PUBLIC – Software engineers shall act consistently with the public interest. 22

23 CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best 23
 24 interests of their client and employer consistent with the public interest. 24

25 PRODUCT – Software engineers shall ensure that their products and related modifications 25
 26 meet the highest professional standards possible. 26

27 JUDGMENT – Software engineers shall maintain integrity and independence in their pro- 27
 28 fessional judgment. 28

29 MANAGEMENT – Software engineering managers and leaders shall subscribe to and pro- 29
 30 mote an ethical approach to the management of software development and maintenance. 30

31 PROFESSION – Software engineers shall advance the integrity and reputation of the pro- 31
 32 fession consistent with the public interest. 32

33 COLLEAGUES – Software engineers shall be fair to and supportive of their colleagues. 33

34 SELF – Software engineers shall participate in lifelong learning regarding the practice of 34
 35 their profession and shall promote an ethical approach to the practice of the profession. 35

36 See [24]. 36
 37 37

38
 39
 40 *IEEE code of ethics* 40
 41 41

42 The Institute of Electrical and Electronics Engineers, IEEE, also has a code of ethics, which 42
 43 is somewhat more explicit. It is found in [7]. 43

44 We, the members of the IEEE, in recognition of the importance of our technologies in affecting 44
 45 the quality of life throughout the world, and in accepting a personal obligation to our profession, 45

1 its members and the communities we serve, do hereby commit ourselves to the highest ethical and
2 professional conduct and agree:

- 3 1. To accept responsibility in making engineering decisions consistent with the safety, health
4 and welfare of the public, and to disclose promptly factors that might endanger the public
5 or the environment;
- 6 2. To avoid real or perceived conflicts of interest whenever possible, and to disclose them to
7 affected parties when they do exist;
- 8 3. To be honest and realistic in stating claims or estimates based on available data;
- 9 4. To reject bribery in all its forms;
- 10 5. To improve the understanding of technology, its appropriate application, and potential con-
11 sequences;
- 12 6. To maintain and improve our technical competence and to undertake technological tasks
13 for others only if qualified by training or experience, or after full disclosure of pertinent
14 limitations;
- 15 7. To seek, accept, and offer honest criticism of technical work, to acknowledge and correct
16 errors, and to credit properly the contributions of others;
- 17 8. To treat fairly all persons regardless of such factors as race, religion, gender, disability, age,
18 or national origin;
- 19 9. To avoid injuring others, their property, reputation, or employment by false or malicious
20 action;
- 21 10. To assist colleagues and co-workers in their professional development and to support them
22 in following this code of ethics.

23 A copy of the code can be downloaded at the IEEE web-site.

24 *SAGE*

25 The System Administrators Guild, SAGE, has its own code of ethics: The System Admin-
26 istrators' Code of Ethics.

27 The SAGE 'vow' is the following: *We as professional System Administrators do hereby*
28 *commit ourselves to the highest standards of ethical and professional conduct, and agree*
29 *to be guided by this code of ethics, and encourage every System Administrator to do the*
30 *same.*

31 The code is found at [20], and contains advice to the system administrator in the form of
32 a vow, for instance, "I will be honest in my professional dealings, and forthcoming about
33 my competence and the impact of my mistakes". The code deals with professionalism, per-
34 sonal integrity, laws and policies, education, and professional and ethical responsibilities. It
35 is interesting to note that the code places emphasis on self-education, especially concern-
36 ing laws, regulations and policies, as well as the responsibility for updating technical knowl-
37 edge and work-related skills. System administrators often lack formal education, and the
38 code makes it clear that every system administrator is personally responsible for acquiring
39 appropriate knowledge of technical, legal and moral matters.

40 *The online ethics center for engineering and science*

41 The online ethics center [12] contains advice on such topics as engineering practice, re-
42 sponsible research, computers and software, diverse workplace, and gives examples of en-
43 gineers and scientists who have behaved wisely in difficult situations. The Center's mission
44 is to provide a forum for the discussion of ethical issues in engineering and science.
45 The Center's mission is to provide a forum for the discussion of ethical issues in engineering and science.

1 is to provide engineers, scientists, and science and engineering students with resources for
 2 understanding and addressing ethically significant problems that arise in their work, and
 3 to serve those who are promoting learning and advancing the understanding of responsible
 4 research and practice in science and engineering [26].

5 The online Ethics also gives guidelines for citation of web-pages, in order to avoid pla-
 6 giarism: *The American Psychological Association's recommendations for citing electronic*
 7 *sources, according to the 5th edition of the APA Publication Manual (2001). Citation of*
 8 *the entire website rather than a specific document requires only the address of the site (i.e.*
 9 *http://onlineethics.org). Citation of a specific document requires the author of the page (if*
 10 *listed), the title of the page, the year the page was created or last modified (found below*
 11 *the left-hand menubar on the graphics version of each page on our site and on the third*
 12 *line of the text version), the title of the website, the date you accessed the page, and the*
 13 *URL.*

14 MLA Guidelines for avoiding plagiarism are found at [12].

15 *The Modern Language Association recommends the following format for citing indi-*
 16 *vidual pages in professional sites on the web. A proper MLA citation should at the least*
 17 *include the author of the page (if listed), the title of the page, the title of the website, the date*
 18 *the page was created or last modified (found below the left-hand menubar on the graphics*
 19 *version of each page on our site and on the third line of the text version), the sponsoring*
 20 *organization, the date you accessed the page, and the URL.*

23 *Ethics Help-Line*

25 The Ethics Help-Line is intended to provide advice for engineers, scientists, and trainees
 26 encountering ethical problems in their work. A principal goal of this Help-Line is to assist
 27 scientists and engineers in maintaining high ethical standards and in acting wisely when
 28 confronted with multiple and potentially conflicting responsibilities, even where this may
 29 lead to conflicts with organizational superiors.

30 The Ethics Help-Line is sponsored by the Online Ethics Center for Engineering and
 31 Science and is cosponsored by the Institute of Electrical and Electronics Engineers (IEEE),
 32 and the National Institute for Engineering Ethics (NIEE) [14].

33 A section of the online ethics center deals with computers and software. *'This section*
 34 *of the OEC contains cases, discussions, and ethical guidelines bearing on the professional*
 35 *responsibilities of computer scientists, computer engineers, and software designers and*
 36 *engineers. These range over fields such as computer theory, computer architecture, and*
 37 *systems engineering'.*

38 One of the scenarios presented explores the ethical issues involved in the electronic
 39 monitoring of the secretarial staff's e-mail [21].

42 **4.3. Whistleblowing**

44 If you discover unethical or illegal actions at work like a violation of law, rule, regulation
 45 or a direct threat to public interest, fraud, health, safety violations and corruption, you must

1 make a decision about what to do with this information. *Whistleblowing* is the term used 1
2 to define an employee's decision to disclose this information to an authority, for instance 2
3 your boss, the media or a government official. 3

4 Whistleblowing takes moral courage. It means acting according to values of right and 4
5 wrong when dominant values decree otherwise, being brave enough to stand up to peo- 5
6 ple who have power, considering and understanding the possible consequences and still 6
7 making the choice to take the action. Despite the dilemmas that potential whistleblowers 7
8 face, there are increasing numbers of people who are prepared to question corrupt or negli- 8
9 gent acts in the workplace, challenging authority by speaking out, even where it may mean 9
10 risking jobs, career or safety to do so. 10

11 12 13 *Whistleblower rights* 13 14

15 Whistleblowers have rights. Courts have awarded whistleblowers their actual wage loss 15
16 until they find another job, the difference between their wages for a reasonable time in 16
17 the future, lost benefits, reinstatement in the previous job, attorney's fees, and punishment, 17
18 damages. The major question is whether and how to blow the whistle. The Public Interest 18
19 Disclosure Act 1998 protects workers who 'blow the whistle' about wrong doing. It applies 19
20 where a worker has a reasonable belief that their disclosure tends to show one or more of 20
21 the following offenses or breaches: 21

- 22 ● A criminal offense. 22
- 23 ● The breach of a legal obligation. 23
- 24 ● A miscarriage of justice. 24
- 25 ● A danger to the health and safety of any individual. 25
- 26 ● Damage to the environment; or 26
- 27 ● Deliberately covering up of information tending to show any of the above. 27

28 Whistleblower protection laws are intended to make it safe for employees to disclose 28
29 company misconduct. Legal protection for whistleblowing varies from country to country. 29
30 In the US, the Office of Special Counsel enforces the whistleblower protection provision 30
31 of the Civil Service Reform Act of 1978, Pub. L. No. 95-454, 92 Stat. 1111 (1979), as 31
32 amended by the Whistleblower Protection Act (WPA) of 1989. The WPA makes it illegal to 32
33 take or threaten to take a *personnel action* against a federal employee because the employee 33
34 has made a protected disclosure. *Personnel action* is broadly defined to include virtually 34
35 any employment-related decision that has an impact on an employee at the worksite. 35

36 In the UK, the Public Interest Disclosure Act 1998 (PIDA) [18]: 36

37 ... provides a framework of legal protection for individuals who disclose information about 37
38 matters of malpractice, and protects whistleblowers from victimisation and dismissal. Under PIDA, 38
39 whistleblowers must use prescribed channels for making disclosures in order to retain the Act's 39
40 protection. The Act's preference is that the disclosure be made to the employer itself or an appro- 40
41 priate public authority, rather than the media. In this manner, the Act protects an employee if he or 41
42 she makes a disclosure in good faith to the employer. 42

43 It is not always easy to determine when whistleblowing may be the right thing to do. 43
44 Informing on illegal or unethical practices in the workplace is difficult for several reasons. 44
45 Ethical justifications for whistleblowing are frequently uncertain. An important question to 45

1 answer is: when is it in the public interest to do so? Whistleblowers should be quite certain
2 of their case before they decide to blow the whistle. 2

3
4
5 *The cases of Inez Austin and Per Yngve Monsen* 5

6
7 Although whistleblowers are protected by law, they may experience great personal strain 7
8 and professional problems, with the loss of work and reputation as a result. They may 8
9 become ostracized and unpopular. 9

10 The online Ethics Center for Engineers and Scientists contains several examples of moral 10
11 conduct. One is the case of the whistleblower Inez Austin, who received the Scientific 11
12 Freedom and Responsibility Award from the American Association for the Advancement 12
13 of Science (AAAS) *for her courageous and persistent efforts to prevent potential safety* 13
14 *hazards involving nuclear waste contamination* as a senior engineer at the Hanford Site in 14
15 Washington state, a 586-square-mile former plutonium production facility. According to 15
16 the AAAS, 16

17 ... her stand in the face of harassment and intimidation reflects the paramount professional duty 17
18 of engineers to protect the public's health and safety and has served as an inspiration to her co- 18
19 workers. 19

20 The Online Ethics Center presents the case of Inez Austin as an example of someone 20
21 who followed her ethical convictions in the face of overwhelming adversity and refused 21
22 to sanction a procedure she believed to be unsafe. In June 1990, Inez Austin refused 22
23 to approve a plan to pump radioactive waste from an aging underground single-shell tank at 23
24 the Hanford Site to a double-shell tank, because she believed that the process was too dan- 24
25 gerous. By blowing the whistle, her life changed, although she came to be regarded highly 25
26 by environmental and ethics groups, she was subjected to a career-destroying combina- 26
27 tion of harassment, bureaucratic maneuvering and ostracization. A second whistleblowing 27
28 incident a few years later led to the loss of her job [13,26]. 28

29 This is the dilemma that a whistleblower must consider. Whistleblowers may be faced 29
30 with harassment and legal pursuit. Although they receive support from media and govern- 30
31 ment, they may later have difficulties finding a job, for who will hire a 'troublemaker?' In 31
32 all probability, many companies have something to hide, and a well-known whistleblower 32
33 is seen as a risk. 33

34 The case of Per Yngve Monsen, the Norwegian employee at Siemens who blew the 34
35 whistle on the company for corruption and financial fraud, demonstrates the hazards a 35
36 whistleblower may be exposed to. He was sacked, and even though he won the court case, 36
37 has been on sick-leave and out of work for nearly two years. In the media he became a hero, 37
38 and like Inez Austin, an example of good moral conduct. But from his experience with a 38
39 powerful company, he advises whistle-blowers to be careful, and give great consideration 39
40 to the risks involved. "If I had known what I know today, I would never have acted like 40
41 I did", is his conclusion, reported by the Norwegian newspaper Aftenposten. The same 41
42 newspaper reported on November the 6th, 2006, that inquiries show that people on the 42
43 whole are afraid to report illegal or unethical activities because of the consequences. 43

44 This is indeed unfortunate, and demonstrates in full that when the individual is up against 44
45 a powerful international company, the results can be disastrous for the person involved. If 45

1 you do discover illegal or unethical behavior, do not hesitate to get in touch with whistle- 1
2 blower protection organizations and receive legal advice before you blow the whistle. 2
3 3
4 4

5 5. Cyber law 5 6 6

7 The phrase *Cyber law* usually refers to rules and laws governing the use of communications 7
8 technology and informations systems. The big challenge regarding this topic is the fact 8
9 that the Internet spans on a world wide basis, while laws typically varies from country to 9
10 country. Also, laws regulating our physical society, are not necessarily sufficient to cover 10
11 all important aspects of cyber space. 11

12 Issues covered by cyber law are: 12

- 13 ● *Intellectual property.* 13
 - 14 ● *Privacy.* 14
 - 15 ● *Freedom of expression.* 15
 - 16 ● *Jurisdiction.* 16
- 17 17
18 18

19 5.1. Intellectual property 19 20 20

21 Intellectual property denotes the specific legal rights which authors, inventors and other IP 21
22 holders may hold and exercise, and not the intellectual work itself [8]. 22

23 *Intellectual property is a legal entitlement which sometimes attaches to the expressed 23
24 form of an idea, or to some other intangible subject matter.* 24

25 The motivation of intellectual property is to protect inventors, authors etc by giving 25
26 them the *ownership* of the result of their brain, similarly to the way people own their 26
27 physical property. The term intellectual property reflects the idea that this subject matter 27
28 is the product of the mind of the intellect, and that intellectual property rights may be 28
29 protected by law in the same way as any other form of property. 29

30 Electronic media and the WWW creates new challenges for the protection of intellectual 30
31 property, and new controversies about how intellectual property law. Some of the prob- 31
32 lems posed by the technology itself are storage and copying of information like text, sound 32
33 and graphics, and the compressed formats like MP3, which makes copying and distribu- 33
34 tion of music simple. Downloading and copying text material from the Internet is simple, 34
35 and makes cheating, for instance, in schools and universities easy. Peer-to-peer technol- 35
36 ogy permits easy transfer of files over the Internet, affecting typically the music and film 36
37 industry [1]. 37

38 Digital Rights Management (DRM) is a technology used by copyright owners to control 38
39 access to digital data. The term often is confused with copy protection, however, DRM 39
40 restrict the actual use of digital content by way of installing the technology as part of 40
41 the design. Today, illegal copying and distribution of copied material can result in severe 41
42 penalties. 42

43 Digital Rights Management is a controversial topic. Copyright holders claim that it is 43
44 their right to restrict copying by the use of technology, because copyright is not respected. 44
45 On the other hand, the Free Software Foundation is a severe critic of DRM, stating that the 45

1 word ‘Rights’ is misleading, and that the term ‘Digital Restrictions Management’ would
 2 be more appropriate. The Electronic Frontier Foundation consider some DRM schemes to
 3 be anti-competitive.

4 We have four main categories of intellectual property; copyright, patents, trade marks
 5 and designs.

8 5.2. Copyright

10 Copyright is a protection that covers published and unpublished literary, scientific and
 11 artistic works, whatever the form of expression, provided such works are fixed in a tangible
 12 or material form. Copyright laws grant the creator the exclusive right to reproduce, prepare
 13 derivative works, distribute, perform and display the work publicly. Copyright protects the
 14 actual piece of work, not the ideas, knowledge or methods used for creating that work.

16 *Copyright gives the creators of a wide range of material, such as literature, art, music,*
 17 *sound recordings, films and broadcasts, economic rights enabling them to control use of*
 18 *their material in a number of ways, such as by making copies, issuing copies to the public,*
 19 *performing in public, broadcasting and use on-line. It also gives moral rights to be iden-*
 20 *tified as the creator of certain kinds of material, and to object to distortion or mutilation*
 21 *of it [8]. Copyright laws enables those who create a piece of work to decide if and how*
 22 *the work can be used, reproduced etc. It is possible to let others use the work freely, or*
 23 *use and distribution must be paid for. There is no such thing as an International Copyright.*
 24 *Protection against unauthorized use in a particular country depends on the national laws of*
 25 *that country. However, most countries do offer protection to foreign works under certain*
 26 *conditions, and these conditions have been greatly simplified by international copyright*
 27 *treaties and conventions. For instance, the Berne Convention for the Protection of Literary*
 28 *and Artistic Works defines the nature and use of intellectual property [2].*

29 Article 2 in the convention defines Protected Works as:

- 30 ● Literary and artistic works.
- 31 ● Possible requirement of fixation.
- 32 ● Derivative works.
- 33 ● Official texts.
- 34 ● Collections.
- 35 ● Works of applied art and industrial designs.
- 36 ● News.

37 According to the convention, *the expression ‘literary and artistic works’ shall include*
 38 *every production in the literary, scientific and artistic domain, whatever may be the mode*
 39 *or form of its expression, such as books, pamphlets and other writings; lectures, addresses,*
 40 *sermons and other works of the same nature; dramatic or dramatico-musical works; chore-*
 41 *ographic works and entertainments in dumb show; musical compositions with or without*
 42 *words; cinematographic works to which are assimilated works expressed by a process*
 43 *analogous to cinematography; works of drawing, painting, architecture, sculpture, en-*
 44 *graving and lithography; photographic works to which are assimilated works expressed*
 45 *by a process analogous to photography; works of applied art; illustrations, maps, plans,*

1 sketches and three-dimensional works relative to geography, topography, architecture or
2 science [2].

3 Copyright laws vary from country to country, but as a rule do not provide less copyright
4 protection than the Berne Convention, as long as the country is a member.

5 Software is not specially mentioned in the convention, but proprietary software is also
6 protected by copyright law. The Software and Information Industry association (SIIA) and
7 the Business Software Alliance (BSA) estimate that the value of pirated software world-
8 wide has been approximately 11–13 billion US dollars per year for many years. Of course
9 these figures are insecure as the activity is illegal, but the gap between the sales number for
10 software licenses and the calculated actual number of applications installed on computers
11 gives some idea of the range of software piracy, as estimated by the SIIA. In China, for
12 instance, dozens of factories are said to produce pirated CDs for export to other countries,
13 even though laws exist to protect intellectual property rights, particularly for foreign work,
14 but the laws are not enforced [1].

17 *Fair use*

18
19
20 There is much discussion about the ethics of copying. A difficult area of copyright law is
21 the so-called ‘Fair Use’. The actual specifics of what is acceptable will be governed by
22 national laws, and although similar, laws will vary from country to country. Cases dealing
23 with fair use can be complex, as decisions are based on individual circumstances and judg-
24 ments. To avoid problems, if in any doubt, it is advised to always get the permission of the
25 owner, prior to use.

26 The UK Copyright Service provides copyright registration for original works by writers,
27 musicians, artists, designers, software providers, authors, companies, organizations and in-
28 dividuals. Known as Copyright Witness internationally, and the UK Copyright Service in
29 the UK, the service supports international copyright protection by securing independent evi-
30 dence that will help prove originality and ownership in any future claims or disputes [27].

31 The UK copyright service defines fair use in the following way: *In copyright law, there*
32 *is a concept of fair use, also known as; free use, fair dealing, or fair practice. Fair use*
33 *sets out certain actions that may be carried out, but would not normally be regarded as*
34 *an infringement of the work. The idea behind this is that if copyright laws are too restric-*
35 *tive, it may stifle free speech, news reporting, or result in disproportionate penalties for*
36 *inconsequential or accidental inclusion.*

37 Under fair use rules, it may be possible to use quotations or excerpts, where the work
38 has been made available to the public (i.e. published). Provided that:

- 39 ● The use is deemed acceptable under the terms of fair dealing.
- 40 ● That the quoted material is justified, and no more than is necessary is included.
- 41 ● That the source of the quoted material is mentioned, along with the name of the author.

42 Typical free uses of work include:

- 43 ● Inclusion for the purpose of news reporting.
- 44 ● Incidental inclusion.
- 45 ● National laws typically allow limited private and educational use.

1 'Incidental inclusion' is where part of a work is unintentionally included. A typical ex- 1
2 ample of this would be a case where holiday movie inadvertently captured part of a copy- 2
3 right work, such as some background music, or a poster that just happened to on a wall in 3
4 the background. 4

5 6 7 *Copyright and the Internet* 7

8
9 The Internet and 'public domain' are not synonymous. Work published on the Internet is 9
10 not automatically placed in the public domain. In the US, material found on the web 10
11 may be copied freely only if the information is created by the federal government, if the 11
12 copyright has expired or the copyright has been abandoned by the holder. 12

13 The following example illustrates the problem: Google is planning to scan books and 13
14 publish them through their service Google Print. This undoubtedly violates copyright pro- 14
15 tection. An author has two rights: The right to create a piece of work, and the right to 15
16 publish that work. Scanning a book means creating copies of that book, and publishing the 16
17 book on the Internet means making copies available for the public. The author must agree 17
18 to this approach, there is no such thing as a silent agreement. Google's arguments are that 18
19 this must be regarded as fair use, but in most European countries, there is no rule which 19
20 makes the copying of books fair use. In all probability, it is not acceptable under US law 20
21 either. Some countries have specific laws defining when it is legal to use parts of published 21
22 work without the author's agreement, for instance for private and educational purposes. 22
23 But making a piece of intellectual property public on the Internet is not covered by any of 23
24 these regulations [28]. 24

25 26 27 **5.3. Patenting** 27

28
29 A patent is related to inventions that are supposed innovative (or new), useful and *non-* 29
30 *obvious*. An inventor may apply for a patent, and after the patent has been issued, the 30
31 patent holder an *exclusive right to commercially exploit the invention for a certain period* 31
32 *of time (typically twenty years from the filing date of a patent application)*. 32

33 A patent gives an inventor the right over the invention for a limited period of time, 33
34 restricting others from copying, selling or using the invention. Most patents today are for 34
35 improvements in known technology. 35

36 Specific conditions must be fulfilled to get a patent. Major ones are that the invention 36
37 must [8] 37

- 38 • Be new or at least undocumented. The invention must not form part of the 'state of the 38
39 art', meaning everything that has been made available to the public before the date of 39
40 applying for the patent. This includes published documents and articles, but also use, 40
41 display, description. 41
- 42 • Involve an inventive step. As well as being new, the invention must not be obvious 42
43 from the state of the art. 43
- 44 • Be industrially applicable. This condition requires that the invention can be made or 44
45 used in any kind of industry. 45

5.4. Trade marks

A trade mark is a distinctive sign which is used to distinguish the products or services of one business from those of another business (Wikipedia).

A trade mark is any sign which can distinguish the goods and services of one trader from those of another. A sign includes words, logos, colours, slogans, three-dimensional shapes and sometimes sounds and gestures. A trade mark is therefore a 'badge' of trade origin. It is used as a marketing tool so that customers can recognise the product of a particular trader. To be registrable in the UK it must also be capable of being represented graphically, that is, in words and/or pictures [8]. Copying a logo or slogan is a violation of copyright law.

5.5. Designs

Design is defined as product appearance, of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture or materials of the product itself or its ornamentation. Design is usually protected by three legal rights: registered designs, unregistered design right and artistic copyright.

Design registration gives the owner a monopoly on their product design, i.e. the right for a limited period to stop others from making, using or selling a product to which the design has been applied, or in which it has been incorporated, without their permission and is additional to any design right or copyright protection that may exist automatically in the design [8].

5.6. Privacy

The Internet with its millions of users, represents several threats to personal security and privacy. Sensitive information is published openly, including telephone conversations, electronic mail, trade secrets and health records. The technological development makes everybody vulnerable to unwanted snooping by governments, business competitors, terrorists, hackers and thieves, in addition to identity theft and fraud. *Privacy International (PI)* is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, DC. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, police information systems, medical privacy, and freedom of information and expression [17].

The protection of privacy is strong in international law. Privacy is a fundamental human right and one of the most important human rights of the modern age. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. Nearly every country in the world includes a right of privacy in its constitution. Modern constitutions include specific rights to access and control one's personal information. International agreements that recognize privacy rights are for instance the International Covenant on Civil and

1 Political Rights or the European Convention on Human Rights (full name: The Convention
2 for the Protection of Human Rights and Fundamental Freedoms, Rome 4 November 1950).
3 Article 8 in this convention states that:

4 Everyone has the right to respect for his private and family life, his home and his correspondence.
5 There shall be no interference by a public authority with the exercise of this right except such as
6 is in accordance with the law and is necessary in a democratic society in the interests of national
7 security, public safety or the economic well-being of the country, for the prevention of disorder or
8 crime, for the protection of health or morals, or for the protection of the rights and freedoms of
9 others.

10 Privacy International (PI) is a human rights group formed in 1990 as a watchdog on
11 surveillance by governments and corporations. PI is based in London, England, and has
12 an office in Washington, DC PI has conducted campaigns throughout the world on issues
13 ranging from wiretapping and national security activities, to ID cards, video surveillance,
14 data matching, police information systems, and medical privacy.

15 Privacy protection is also controlled by individual users. Internet users employ various
16 programs and systems that provide privacy and security of communications. These include
17 encryption, anonymous remailers, proxy servers and digital cash. Not all tools effectively
18 protect privacy [17].
19
20

21 *Phil Zimmermann and PGP – Pretty Good Privacy*

22
23 Philip R. Zimmermann is the creator of Pretty Good Privacy, an email encryption soft-
24 ware package. Zimmermann, a software engineer with more than 20 years of experience in
25 cryptography and data security originally designed PGP as designed as a human rights tool,
26 and published it for free on the Internet in 1991. As a consequence, Zimmermann was sub-
27 jected to three years of criminal investigation, because the US government maintained that
28 US export restrictions for cryptographic software were violated when PGP spread world-
29 wide. However, the government dropped the case in 1991, and PGP has since become the
30 most popular email encryption software in the world. Zimmermann founded PGP Inc. in
31 1991, a company that was acquired by Network Associates Inc (NAI) in December 1997.
32 In 2002 PGP was acquired from NAI by a new company called PGP Corporation. Zimmer-
33 mann is now a consultant for companies and industry on cryptography. His home page is
34 found at <http://www.philzimmermann.com/>.
35
36

37 **5.7. Privacy and Human Rights**

38
39 The Universal Declaration of Human Rights from 1948 article 12 states that “*No one shall*
40 *be subjected to arbitrary interference with his privacy, family, home or correspondence,*
41 *nor to attacks upon his honour and reputation. Everyone has the right to the protection of*
42 *the law against such interference or attacks*”.

43 According to the International Covenant on Civil and Political Rights – 1966 article 17:

- 44 1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, fam-*
45 *ily, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

Public information is defined as information knowable by all, for instance information you have provided to an organization that has a right to share it with other organizations. An example of such information is the telephone directory. On the other hand, personal information is not part of a public record, for example your religious and political beliefs. If you personally disclose this information to an organization with the right to inform other organizations, it becomes public information.

5.8. Oversight and privacy

In countries with a data protection or privacy act, there is an official or agency that oversees enforcement of the act. The powers of these officials, Commissioner, Ombudsman or Registrar, vary by country. Several countries, including Germany and Canada, also have officials or offices on a state or provincial level.

Under Article 28 of the EU Data Protection Directive, all European Union countries must have an independent enforcement body [4]. Under the Directive, these agencies are given considerable power: governments must consult the body when the government draws up legislation relating to the processing of personal information; the bodies also have the power to conduct investigations and have a right to access information relevant to their investigations; impose remedies such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports. Several countries that do not have a comprehensive act still have a commissioner. A major power of these officials is to focus public attention on problem areas, even when they do not have any authority to fix the problem. They can do this by promoting codes of practice and encouraging industry associations to adopt them. They also can use their annual reports to point out problems. For example, in Canada, the Federal Privacy Commissioner announced in his 2000 report the existence of an extensive database maintained by the federal government. Once the issue became public, the Ministry disbanded the database.

5.9. Freedom of speech on the Internet: the role of freenet

The Internet is a powerful and positive forum for free expression. Internet users, online publishers, library and academic groups and free speech and journalistic organizations share a common interest in opposing the adoption of techniques and standards that could limit the vibrance and openness of the Internet as a communications medium. Indeed, content 'filtering' techniques already have been implemented in ways inconsistent with free speech principles, impeding the ability of Internet users to publish and receive constitutionally protected expression [9].

Article 19 of the Universal Declaration of Human Rights and Article 10 of the European Convention on Human Rights are international human rights proclamations that support the freedom of speech, although implementation of this fundamental human right is unfortunately lacking in many countries. However, the right to freedom of speech is not unlimited, many governments may prohibit certain forms of expression. According to international

1 law, restrictions on free speech must be provided by law, pursue an aim recognized as leg- 1
2 gitimate, and be necessary for the accomplishment of that aim. Some of the aims that are 2
3 considered legitimate are protection of the rights and reputations of others and the pro- 3
4 tection of national security and public order, health and morals. There are differences of 4
5 opinion among people of different nations and cultures as to when restriction of free speech 5
6 meets these criteria [31]. 6

7 The Internet has opened new possibilities for achieving freedom of speech, giving 7
8 anybody the opportunity to publish whatever they want independent of legal measures. 8
9 Pseudonymity and data havens (such as Freenet [6]) allow unlimited free speech, because 9
10 the technology guarantees that material cannot be removed or censored. 10

11 Freenet is free software which lets you publish and obtain information on the Internet without fear 11
12 of censorship. To achieve this freedom, the network is entirely decentralized and publishers and 12
13 consumers of information are anonymous. Without anonymity there can never be true freedom of 13
14 speech, and without decentralization the network will be vulnerable to attack. 14

15 Communications by Freenet nodes are encrypted and are routed through other nodes to 15
16 make it extremely difficult to determine who is requesting the information and what its 16
17 content is. Users contribute to the network by giving bandwidth and a portion of their hard 17
18 drive (called the 'data store') for storing files. Unlike other peer-to-peer file sharing 18
19 networks, Freenet does not let the user control what is stored in the data store. Instead, files are 19
20 kept or deleted depending on how popular they are, with the least popular being discarded 20
21 to make way for newer or more popular content. Files in the data store are encrypted to 21
22 reduce the likelihood of prosecution by persons wishing to censor content. 22

23 Websites which are censored by national governments are often re-hosted on a server in 23
24 a country with no censorship restrictions. The United States has in many ways the world's 24
25 least restrictive governmental policies on freedom of speech. Many websites re-host their 25
26 content on an American server to escape censorship. This is especially the case with neo- 26
27 nazi and other sites promoting racial hatred, since these are illegal in many European coun- 27
28 tries. 28

29 Another organization dedicated to protecting freedom of speech on the Internet is The 29
30 Electronic Frontier Foundation (EFF), found at www.eff.org. The '*EFF is a donor-funded* 30
31 *nonprofit and depends on your support to continue successfully defending your digital* 31
32 *rights. Litigation is particularly expensive; because two-thirds of our budget comes from* 32
33 *individual donors, every contribution is critical to helping EFF fight, and win, more cases.'* 33
34 34

35 5.10. Google and China 35

36 36
37 37
38 38
39 The Chinese government has imposed Internet censorship in order to control or eliminate 39
40 access to information on controversial and sensitive topics such as the Tiananmen Square 40
41 protests of 1989, Falun Gong, Tibet, Taiwan, pornography or democracy. They have also 41
42 enlisted the help of some American companies like MSN, who have subsequently been 42
43 criticized by proponents of freedom of speech. 43

44 Online search giant Google launched a China-based search engine that will be self- 44
45 censored to avoid posting results that antagonize China's communist government. 45

1 Google.cn uses the Chinese Web suffix *.cn* in addition to the existing Chinese-language
2 Google website hosted on servers in the USA.

3 In order to operate from China, we have removed some content from the search results available on
4 Google.cn, in response to local law, regulation or policy. Removing search results is inconsistent
5 with Google's mission, but providing no information is more inconsistent with our mission.

6 Senior policy counsel Andrew McLaughlin, Google.

7
8 The Google mirror *elGoog* makes it possible to search for words like 'democracy' from
9 inside China. <http://elgoog.rb-hosting.de/index.cgi>.

12 5.11. Transborder data flows

14 Data protection laws can be circumvented by transferring personal information to third
15 countries, where the national law of certain countries do not apply. The data can then be
16 processed in these countries, called 'data havens'. This is why most data protection laws
17 include restrictions on the transfer of information to third countries unless the information
18 is protected in the destination country. For example, Article 12 of the Council of Europe's
19 1981 Convention places restrictions on the transborder flows of personal data [4]. Similarly,
20 Article 25 of the European Directive imposes an obligation on member States to ensure
21 that any personal information relating to European citizens is protected by law when it is
22 exported to countries outside Europe. It states:

23 The Member States shall provide that the transfer to a third country of personal data which are
24 undergoing processing or are intended for processing after transfer may take place only if the third
25 country in question ensures an adequate level of protection.

26
27 Therefore, there is currently growing pressure outside Europe for the passage of strong
28 data protection laws. Those countries that refuse to adopt privacy laws may be unable to
29 conduct certain types of information flows with Europe, particularly if they involve sen-
30 sitive data. The European Commission determines a third country's system for protecting
31 privacy, where the main principle in this determination process is that the level of protec-
32 tion in the receiving country must be *adequate* rather than *equivalent*. In this way, privacy
33 protection is guaranteed from the third party, although the precise dictates of the Directive
34 are not strictly followed.

37 6. Educational aspects

39 6.1. Teaching ethics

41 In order for computer professionals to incorporate an *ethical responsibility*, it has been
42 stressed that it is important to have this topic introduced to them already during their edu-
43 cational years.

44 As system administration is not a common educational programme yet, most of the
45 topics on this issue have been inspired by the more general field of Computer Science

1 and Information Systems. However, most of these issues are also relevant for the system
2 administration education.

3 There has been significant controversy in the field of teaching ethics to computer science
4 graduates. There have been debates on all imaginable aspects of the issue, on what kind
5 of *subjects* should be covered by the curriculum, *how* the material should be integrated
6 (separate course or modules in other courses), and *who* should actually teach these subjects:

7 However, *how* to incorporate social and ethical aspects into the technical programmes
8 has not proven trivial. Common problems have been:

- 9 • *What* should the students learn?
- 10 • *Who* should teach these untraditional subjects?
- 11 • *How* should these issues be integrated in the traditional curriculum?

12
13
14 *Course content and learning objectives* The *ACM/IEEE Computing Curriculum 1991*,
15 demanded an inclusion of ethical and social aspects in the Computer Science curriculum,
16 therefore, the project *ImpactCS* was funded [25]. The objective of this project was to define
17 the core content and develop a framework for integrating social and ethical topics into the
18 computer science curriculum [29].

19 The project delivered three reports [11], where each of them covered different aspects
20 of the process of including ethics in the CS curriculum. Among the final results was a very
21 broad list of topics, which included the following *learning objectives*:

- 22 • *Responsibility of the Computer Professional for Computer Science*. This topic again
23 contains the subtopics:
24 – History of the development and impact of computer technology.
25 – Why be ethical?
26 – Major ethical models.
27 – Definition of computing as a profession.
- 28 • *Basic Elements of Ethical Analysis for Computer Science*. The elements covered by
29 this section are:
30 – Ethical claims can and should be discussed rationally.
31 – Ethical choices cannot be avoided.
32 – Easy ethical approaches are questionable.
- 33 • *Basic Skills of Ethical Analysis for Computer Science*:
34 – Arguing from example, analogy, and counter-example.
35 – Identifying stakeholders in concrete situations.
36 – Identifying ethical issues in concrete situations.
37 – Applying ethical codes to concrete situations.
38 – Identifying and evaluating alternative courses of action.
- 39 • *Basic elements of Social Analysis for Computer Science*:
40 – Social context influences the development and use of technology.
41 – Power relations are central in all social interactions.
42 – Technology embodies the values of the developers.
43 – Populations are always diverse.
44 – Empirical data are crucial to design and development processes.

- *Basic Skills of Social Analysis for Computer Science:*

- Identifying and interpreting the social context of a particular system.
- Identifying assumptions and values embedded in a particular system.
- Using empirical data to evaluate a particular implementation of a technology.

As the list shows, the project ImpactCS provides a very broad range of subjects, not supported by all members of this community. David Preston claims this list is too long, and that most of the subjects are out of scope for an ethics course to be interesting for the Computer Science students [16]. A more narrow approach is recommended, to assure better relevance and hence interest from the students. In particular, they recommend spending considerable time focusing on the students' *own* experiences, as these tend to arouse more interest and participation among the students.

6.2. How should professional ethics be taught?

After establishing the learning objectives, there is still the issue of how to determine the teaching form for this kind of material. Using *case studies* is a very common approach, as this is claimed to improve the understanding of certain ethical dilemmas and increase interest and hence participation among the students. Some authors object to this, with the argument that case studies do not bring sufficient realism to the issues, and that the students should be encouraged to bring their *own* experiences to class [16].

The form of the lectures is also heavily debated, although it seems to be agreed upon that a mixture of *group discussions*, *guest lectures*, student-prepared *panel debates* and so on, is to be preferred over more traditional teacher-led lectures. One particular issue is whether the communication between teacher and students should be *one-way*, or if it should be more negotiation-based. Regarding so-called *open sessions*, where external speakers give talks with interaction with the students, there seem to be very difficult to predict which topics appeal to the students.

There is also significant emphasis on using a variety of technical resources in the classes, for instance local, national or international newspapers, local leaflets, film, music, student-generated material, fiction etc.

Who should teach ethics? One of the problems with integrating an ethics and social aspects course in the computer science or system administration curriculum, is the lack of knowledge of the teachers and faculty. The discussion has been about who should teach these subjects: faculty of engineering or teachers of philosophy or social science.

The clear advantage of having teachers from the computer science community teach computer ethics is that they are familiar with the technological aspects of the use of computers, and the work situations in which ethical dilemmas arise. The use of case studies from industry is a recommended approach, and computer professionals have first-hand knowledge of the issues that are described in well-known cases and examples. Teachers of Philosophy may tend to present ethical theory and cases in a too theoretical and academic manner, which may have little relevance for computer professionals.

6.3. Teaching students to hack: a necessity or security risk?

The emergence of diverse security threats has led to increased focus on information security courses in the computer science education. A significant part of such courses has been the *security labs*, where students can achieve hands-on experience with important tools and concepts within information security, both regarding potential threats and how to protect the systems from diverse attacks [10].

Typical student activities in these labs are:

1. Hacking (accessing systems or networks where the students do not have access).
2. Find vulnerable systems and penetrate them.
3. Remove evidence of penetration.

The argument for teaching the students such skills have been that the system administrators must possess the same skills as the attackers in order to be able to protect the system from the attacks (know your enemy). The reason for this is mainly the need for so-called *ethical hackers*.

The term *ethical hacking* comes from the practice of skilled ‘hackers’ trying to break into computer systems with the goal of discovering potential vulnerabilities in the system, in order to prevent attacks. More precisely, the ethical hackers aim at answering the following questions [15]:

- What part of the system is visible to an intruder?
- What can an intruder do with that information?
- Does anyone at the target notice the intruder’s activities?

Arguments in favor of this practice has been [10]:

- “that hacking skills are equivalent to audit skills as both are designed to discover flaws in the protection of data and secure operation of a system. Just as auditors test systems for security or operational flaws, hackers ‘test’ systems through attack;
- Knowledge of hacking skills and practice in attacking secured systems improves security by informing network administrators of how an exploit can be executed; and
- To provide the best security defense, a systems administrator must possess the same skills as the attacker”.

This kind of work obviously requires people with significant skills and experience, which has led to several universities and colleges including ‘hacking’ exercises as part of their computer security curriculum. Examples of such exercises have been writing port scanners, propagating viruses and exploit programs, in addition to activities like packet sniffing and injecting packets.

However, recently there has been increased focus on the downsides of this kind of organized student activity. There obviously is a significant risk of actually *educating* hackers or the ‘bad guys’. Further, hacking skills does not necessarily make system administrators able to prevent such attacks.

To avoid malicious behavior from students, some universities offer security labs only at the graduate level, with the motivation that only the most mature, and hence more responsible students will have access to this kind of information. Other universities have tried avoiding hands-on content or keeping the labs away from student access.

These methods have proved to have weaknesses, so as alternative methods for educating the students, the following has been suggested [10]:

- 1 ● Teaching recovery activities. 1
- 2 ● Intensive vulnerability assessments of a simulated corporate network. 2
- 3 ● Network forensic investigations. 3
- 4 The following questions are asked by the authors of [10]: 4
- 5 ● How should students be taught to implement network and desktop security? 5
- 6 ● Is hacking and virus-writing a pre-requisite for developing strong technical skills in 6
7 detecting malicious activity? 7
- 8 ● What course content (if any) should be off-limits? 8
- 9 ● Will hacking skills for network administrators necessarily improve security and their 9
10 employability? 10

13 7. Summary 13

14 15 The use of computers and computer networks poses ethical questions that often differ from 15
16 our every-day ethical problems, mainly because of the nature of the technology itself. 16
17 Computers have become universal tools, computers and networks are everywhere, shap- 17
18 ing our lives, work and leisure time. With the rapid development of computer technology, 18
19 new situations constantly arise and create policy vacuums, because the answers to ethi- 19
20 cal dilemmas are not clear. The law will not always be a help, because laws are designed 20
21 to fit the technologies and problems of the day, and because technology is developing at 21
22 such a tremendous speed. It takes time for the legal issues to catch up with the technical 22
23 possibilities. 23

24 System administrators are often faced with ethical dilemmas in situations where they 24
25 must make decisions, and take proper action. There are many paths to becoming a system 25
26 administrator, and many lack formal education. Decisions may therefore often be founded 26
27 on intuition, or be taken under pressure. The consequences can be serious, like the risk of 27
28 losing a job, either through negligence, or because of being pressured into some illegal or 28
29 unethical activity. For a system administrator it is therefore of the greatest importance to be 29
30 acquainted with the rules, laws and policies regarding the performance of the work duties. 30

31 A system administrator must be able to make sound decisions based on reflection, 31
32 knowledge, common sense and professional responsibility, and is, according to the sage 32
33 code of Ethics, also obliged to educate himself/herself on technical, legal and ethical is- 33
34 sues. In this chapter we have sought to outline some of the most important laws, ethical 34
35 principles and guidelines that may assist the system administrator in fulfilling his or her 35
36 professional duties. 36

39 References 39

- 40 40
- 41 [1] S. Baase, *A Gift of Fire*, Pearson Education (2003). 41
- 42 [2] *Berne Convention for the Protection of Literary and Artistic Works*, http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html. 42
- 43 [3] P.N. Edwards, C.A. Lee and B.S. Williams, *Evaluating informations and communications technology: Per- 43
44 spectives for a balanced approach* (2001). 44
- 45 [4] *EU Data Protection Directive*, <http://www.opsi.gov.uk/ACTS/acts1998/19980023.htm>. 45

- 1 [5] **Free Software Foundation (FSF)**, <http://www.fsf.org/>. 1
- 2 [6] **Freenet project**, <http://freenetproject.org/> (2006). 2
- 3 [7] **IEEE**, *Code of ethics*, <http://www.ieee.org/portal/pages/about/whatis/code.html>. 3
- 4 [8] **Intellectual Property**, <http://www.intellectual-property.gov.uk/index.html>. 4
- 5 [9] **Internet Free Expression Alliance**, <http://www.ifea.net>. 5
- 6 [10] **P.Y. Logan and A. Clarkson**, *Teaching students to hack: Curriculum issues in information security*, SIGCSE, 6
ACM (2005). 6
- 7 [11] **C.D. Martin and E. Yale Wertz**, *From awareness to action: Integrating ethics and social responsibility into 7
the computer science curriculum*, Computers and Society (1999). 7
- 8 [12] **Online Ethics Centre**, <http://onlineethics.org/cite-link.html> (2006). 8
- 9 [13] **Online Ethics Centre**, <http://onlineethics.org/moral/austin/index.html> (2006). 9
- 10 [14] **Online Ethics Helpline**, <http://onlineethics.org/helpline/index.html> (2006). 10
- 11 [15] **C.C. Palmer**, *Ethical hacking*, <http://www.research.ibm.com/journal/sj/403/palmer.html> (2001). 11
- 12 [16] **D. Preston**, *What makes professionals so difficult: An investigation into professional ethics teaching*, Pro- 12
ceedings of POLICY'98: Ethics and Social Impact, ACM Press (1998). 12
- 13 [17] **Privacy International**, <http://www.privacyinternational.org>. 13
- 14 [18] **Protection for Whistleblowers**, <http://www.ignet.gov/randp/f01c10.pdf>. 14
- 15 [19] **M.J. Quinn**, *Ethics for the Information Age*, Pearson Education (2006). 15
- 16 [20] **SAGE**, *Code of ethics*, <http://www.sage.org/ethics>. 16
- 17 [21] **Scenarios about computers and software**, <http://onlineethics.org/com/scenarios.html>. 17
- 18 [22] **J.P. Sterba**, *Ethics: The Big Questions*, Blackwell Publishers (2002). 18
- 19 [23] **Suggested Guidelines for Writing a Code of Ethics/Conduct**, [http://www.deloitte.com/dtt/cda/doc/content/ 19
Suggested%20Guidelines%20for%20writing%20a%20code%20of%20ethics%2C%20conduct.pdf](http://www.deloitte.com/dtt/cda/doc/content/Suggested%20Guidelines%20for%20writing%20a%20code%20of%20ethics%2C%20conduct.pdf). 19
- 20 [24] **The ACM Software Engineering Code of Ethics and Professional Practice**, [http://www.acm.org/ 20
constitution/code.html](http://www.acm.org/ 20
constitution/code.html). 20
- 21 [25] **The ImpactCS Home Page**, <http://www.seas.gwu.edu/impactcs/>. 21
- 22 [26] **The Online Ethics Center for Engineering and Science**, <http://www.onlineethics.org>. 22
- 23 [27] **The UK Copyright Service**, <http://www.copyrightservice.co.uk/>. 23
- 24 [28] **O. Torvund**, *Copyright: An introduction – (Norwegian)*, <http://www.torvund.net/artikler/art-opphav.asp>. 24
- 25 [29] **L.H. Werth**, *Getting started with computer ethics*. Proceedings of the Twenty-Eighth SIGCSE Technical 25
Symposium on Computer Science Education, ACM Press (1997), 1–5. 25
- 26 [30] **Wikipedia**, 13.08.2006. <http://www.wikipedia.org>. 26
- 27 [31] **Wikipedia**, http://en.wikipedia.org/wiki/Freedom_of_speech. 27
- 28 28
- 29 29
- 30 30
- 31 31
- 32 32
- 33 33
- 34 34
- 35 35
- 36 36
- 37 37
- 38 38
- 39 39
- 40 40
- 41 41
- 42 42
- 43 43
- 44 44
- 45 45