1 Morality

1. Directives that guide our conduct as individuals
2. Social policies framed at the macrolevel

Moral systems are evaluated against standards called *principles*. Morality is:

Public Rules are public; Everyone is obligated to partake in a moral system

Informal Has no formal authoritative judges presiding over it

Impartial Moral rules are ideally designed to apply equitably to all participants

Rational The system is based on principles of logical reason

2 Values

Instrumental Provide external benefit (eg. computers etc)

Intrinsic Valued for their own sake (eg. life, happiness)

3 Ethical Theories

3.1 Consequence-based (Utilitarianism)

Some have argued that the primary goal of a moral system is to produce desirable consequences or outcomes for its members. For these ethicists, the consequences (i.e., the ends achieved) of actions and policies provide the ultimate standard against which moral decisions must be evaluated

3.1.1 Utilitarianism

> An individual act (X) or a social policy (Y) is morally permissible if the consequences that result from (X) or (Y) produce the greatest amount of good for the greatest number of persons affected by the act or policy.

1. Social utility is superior to alternative criteria for evaluating moral systems.
2. Social utility can be measured by the amount of happiness produced.

Assumes:

1. All people desire happiness.
2. Happiness is an intrinsic good that is desired for its own sake.

Act Utilitarianism:

> An act, X, is morally permissible if the consequences produced by doing X result in the greatest good for the greatest number of persons affected by Act X.

Rule Utilitarianism:

> An act, X, is morally permissible if the consequences of following the general rule, Y, of which act X is an instance, would bring about the greatest good for the greatest number.

Critic against Utilitarianism:

1. Morality is basically tied to the production of happiness or pleasure.
2. Morality can ultimately be decided by consequences (of either acts or policies).

Critics of utilitarianism argue that morality can be grounded neither in consequences

3.2 Duty-based (Deontology)

Kant points out that, in some instances, performing our duties may result in our being unhappy and may not necessarily lead to consequences that are considered desirable.

Kant bases deontology on two premises:

1. Our nature as rational creatures
    - Rationality is what separates us from other kinds of creatures. If our primary nature were to merely seek happiness or pleasure, we would be indistinguishable from other creatures.
    - Rational nature reveals certain duties or obligations to each other as "rational beings"
2. Human beings are ends-in-themselves
    - A genuinely moral system would never permit some humans to be treated as means to the ends of others
    - We have a duty to treat fellow humans as ends; each individual has the same moral worth

Categorical Imperative:

> Act always on that maxim or principle (or rule) that can be universally binding, without exception, for all human beings.

This forms a system of universality and impartiality. The objective rule to be followedthat is, the litmus test for determining when an action will have moral worthis whether the act complies with the categorical imperative, and whether it is universal and impartial.

Act Deontology:

Ross argues that when two or more moral duties clash, we have to look at individual situations in order to determine which duty will override another.

Ross believes that we have certain prima facie (or self-evident) duties, which, all things being equal, we must follow. He provides a list of prima facie duties such as honesty, benevolence, justice, and so forth.

1. Reflect on the competing prima facie duties.
2. Weigh the evidence at hand to determine which course of action would be required in a particular circumstance.

3.3 Contract-based

In his classic work *Leviathan*, Hobbes describes an original "premoral" state that he calls the "state of nature." It is premoral because there are no moral (or legal) rules yet in existence. In this state, each individual is free to act in ways that satisfy his or her own natural desires. According to Hobbes, our natural (or physical) constitution is such that in the state of nature we act in ways that will enable us to satisfy our desires (or appetites) and to avoid what Hobbes calls our "aversions."

Hobbes believes that we are willing to surrender some of our "absolute" freedoms to a sovereign. In return, we receive many benefits, including a system of rules and laws that are designed and enforced to protect individuals from being harmed by other members of the system.

We see that it is in our individual self-interest to develop a moral system with rules.

3.3.1 Criticisms

Some critics, such as Pojman (2006), point out that contract-based theories provide the foundation for only a minimalist morality. They are minimalist in the sense that we are obligated to behave morally only where an explicit or formal contract exists. So if I have no express contract with you, or if a country such as the United States has no explicit contract with a developing nation, there is no moral obligation for me to help you or for the United States to come to the aid of that developing nation.

3.4 Rights-Based

- humans possess some natural rights
- Two kinds of legal rights: positive rights and negative rights. Having a negative right to something simply means that one has the right not to be interfered with in carrying out the privileges associated with that right.
- Positive rights more rare and harder to justify.

3.5 Character-based

Because virtue ethics focuses primarily on character development and moral education, it does not need to rely on a system of formal rules.

Character-based ethical systems would most likely flourish in cultures where the emphasis placed on community life is stronger than that accorded to the role of individuals themselves.

Type of Theory	Advantages	Disadvantages
Consequence-based (Utilitarian)	Stresses promotion of happiness and utility	Ignores concerns of justice for the minority population
Duty-based (deontology)	Stresses the role of duty and respect for persons	Underestimates the importance of happiness and social utility
Contract-based (rights)	Provides a motivation for morality	Ofers only a minimal morality
Character-based (virtue)	Stresses character development and moral education	Depends on homogeneous standards for morality

3.6 Moor's Just Consequentialist Framework

1. Deliberate over various policies from an impartial point of view to determine whether they meet the criteria for being ethical policies. A policy is ethical, if it
   - does not cause any unnecessary harms to individuals and groups, and
   - supports individual rights, the fulfilling of duties, etc.
2. Select the best policy from the set of just policies arrived at in the deliberation stage by ranking ethical policies in terms of benefits and (justifiable) harms. In doing this, be sure to:
   - weigh carefully between the good consequences and bad consequences in the ethical policies, and
   - distinguish between disagreements about facts and disagreements about principles and values, when deciding which particular ethical policy should be adopted. (Knowledge about the facts surrounding a particular case should inform the decision-making process.)

4 Professional Ethics

Professionals are experts in a field, which provides them an advantage over the lay person and that professionals work has the potential to impacteither positively or negativelythe general public at large.

Broadly speaking, a computer/IT professional is anyone employed in the computing and IT fieldsfrom software and hardware engineers, to specialists such as support person- nel, network administrators, and computer repair technicians.

As IT professionals we have significant opportunities to:

1. do good or cause harm,
2. enable others to do good or cause harm,
3. influence others to do good or cause harm.

Moral Responsibility determined by looking at causality and intent. X is responsible for Y if X caused Y, regardless of intention of outcome, or regardless of the outcome of an intention.

Legal Liability usually a legal concept, determines compensation for harmful consequences, rather than blame. May be legally liable, though not morally responsible

Accountability Broader concept than liability that finds answerable to superiors, authorities, or public. Helps because responsibility is hard to pinpoint to individuals in large software developments.

4.1 Whistleblowing

Morally permitted to blow the whistle:

1. The product will do "serious and considerable harm" to the public.
2. The engineer(s) have reported the "serious threat" to their immediate supervisor.
3. The engineer(s) have "exhausted the internal procedures and possibilities" within the company, including going to the board of directors, having received no support from their immediate supervisor.

To have a strict moral obligation to blow the whistle, De George believes that two additional conditions must be satisfied:

1. The engineer(s) have "accessible, documented evidence that would convince a reasonable, impartial, observer that ones view of the situation is correct."
2. The engineer(s) have "good reasons to believe that by going public the necessary changes will be brought about."

5 Privacy

Consider the impact that changes involving this technology have had on privacy with respect to the:

1. amount of personal information that can be collect,
2. speed at which personal information can be transmitted,
3. duration of time that the information can be retained,
4. kind of information that can be acquired and exchanged.

5.1 Definitions

Accessibility privacy Privacy is defined as ones physically being let alone, or being free from intrusion into ones physical space.

Decisional privacy Privacy is defined as freedom from interference in ones choices and decisions.

Informational privacy Privacy is defined as control over the flow of ones personal information, including the transfer and exchange of that information.

5.2 Moor's Account of Privacy

> An individual [has] privacy in a situation with regard to others if and only if in that situation the individual [is] protected from intrusion, interference, and information access by others.

5.2.1 Naturally private vs normatively private

In a naturally private situation, individuals are protected from access and interference from others by natural means, for example, physical boundaries such as those one enjoys while hiking alone in the woods. In this case, privacy can be lost but not violated, because there are no normsconventional, legal, or ethicalaccording to which one has a right, or even an expectation, to be protected. In a normatively private situation, on the other hand, individuals are protected by conventional norms (e.g., formal laws and informal policies) because they involve certain kinds of zones or contexts that we have determined to need normative protection.

5.3 Contextual Integrity

Nissenbaums privacy framework requires that the processes used in gathering and disseminating information (a) are "appropriate to a particular context" and (b) comply with norms that govern the flow of personal information in a given context. She refers to these two types of informational norms as follows:

1. Norms of appropriateness.
2. Norms of distribution.

Whereas norms of appropriateness determine whether a given type of personal information is either appropriate or inappropriate to divulge within a particular context, norms of distribution restrict or limit the flow of information within and across contexts. When either norm has been "breached," a violation of privacy occurs; conversely, the contextual integrity of the flow of personal information is maintained when both kinds of norms are "respected."

5.4 The Value of Privacy

Fried suggests that unlike most instrumental values that are simply one means among others for achieving a desired end, privacy is also essential, that is, necessary to achieve some important human ends, such as trust and friendship. We tend to associate intrinsic values with necessary conditions and instrumental values with contingent, or nonnecessary conditions; so while privacy is instrumental in that it is a means to certain human ends, Fried argues that it is also a necessary condition for achieving those ends.

Moor believes that privacy is an articulation, or "expression" of the "core value" security, which in turn is essential across cultures, for human flourishing.

Based on the insights of DeCew and others, one might infer that privacy is a value that simply benefits individuals. However, some authors have pointed out the social value that privacy also provides, noting that privacy is essential for democracy.

6 Security

Type	What
Data	Securing data that resides in computer databases; transmitted between computer systems
System	Securing hardware and operating system resources; application software and programs
Network	Securing the infrastructure of privately owned networks; infrastructure of the Internet

Data security Concerned with vulnerabilities pertaining to unauthorized access to data, as well as with threats to the confidentiality, integrity, and availability of data that resides in computer storage devices or is exchanged between computer systems. Data can either be sensitive, or proprietary, or both.

Confidentiality Preventing unauthorized persons from gaining access to unauthorized information

Integrity Preventing an attacker from modifying data.

Accessibility Making sure that resources are available for authorized users.

System security Concerned with attacks on system resources (such as computer hardware, operating system software, and application software) by malicious programs.

Network security Concerned with attacks on computer networks, including the infrastructure of privately owned networks as well as the Internet itself.

6.1 Difference between privacy and security

Privacy Personal info accessed by organisations claiming to have legitimate need

Security Obtaining of information by unauthorised personnel

Privacy can obscure the identity of security violaters

6.2 Cloud Computing

a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services).

6.2.1 Major Concerns

1. How users can control their data stored in the cloudcurrently, users have very little "control over or direct knowledge about how their information is transmitted, processed, or stored".
2. Integrity of the data - for example, if the host company goes out of business, what happens to the users data?
3. Access to the data; i.e., can the host deny a user access to his/her own data?
4. And a fourth concern has to do with who actually "owns" the data that is stored in the cloud

6.3 Hacking and Hacker Ethic

According to Simpson (2006), a hacker is anyone who "accesses a computer system or network without authorization from the owner."

Steven Levy (2001)

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authoritypromote decentralization.
4. Hackers should be judged by their hacking (not by bogus criteria such as degrees, age, race, or position).
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

6.4 Cyberterrorism

Dorothy Denning (2004) defines it as the convergence of terrorism and cyberspace. As such, cyberterrorism covers politically motivated hacking operations intended to cause grave harmthat is, resulting in either loss of life or severe economic loss, or both.

6.5 Hacktivism

"Electronic Civil Disobedience" (ECD). Criteria for CD:

1. No damage done to persons or property. (Debatable, depending on context)
2. Nonviolent.

3. Not for personal profit.
4. Ethical motivationthe strong conviction that a law is unjust, or unfair, to the extreme detriment of the common good.
5. Willingness to accept personal responsibility for the outcome of actions.

Hacktivism The convergence of political activism and computer hacking techniques to engage in a new form of civil disobedience.

Cyberterrorism The convergence of cybertechnology and terrorism for carrying out acts of terror in (or via) cyberspace.

Information Warfare Using malware in cyberattacks designed to mislead the enemy and disrupt/damage an opponents military defense system and its critical infrastructure.

7 Cybercrime

By thinking about cybercrimes in terms of their unique or special featuresi.e., conditions that separate them from ordinary crimeswe could distinguish authentic or genuine cybercrimes from other crimes that merely involve the use or the presence of cybertechnology. We propose a definition of a genuine cybercrime as a crime in which

> the criminal act can be carried out only through the use of cybertechnology and can take place only in the cyberrealm.

Cyberpiracy using cybertechnology in unauthorized ways to (a) reproduce copies of proprietary information, or (b) distribute proprietary information (in digital form) across a computer network.

Cybertrespass using cybertechnology to gain unauthorized access to (a) an individuals or an organizations computer system, or (b) a password-protected Web site.

Cybervandalism using cybertechnology to unleash one or more programs that (a) disrupt the transmission of electronic information across one or more computer networks, including the Internet, or (b) destroy data resident in a computer or damage a computer systems resources, or both.

7.1 Pre-emptive hacking

> The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits ... an Ethical Hacker is very similar to a Penetration Tester ... When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal.

Justified through utilitarian/consequentialist means Less harm overall, society gain benefits from a more robust system

Not justified as innocent individuals are used as means to an end The systems of innocent users are used for pre- emptive hacking as 'host computers', which is morally unjustifiable under deontological theory, as nobody should be used as an means to an end

7.2 Cyber-assisted crimes

Cyberexacerbated Cyberstalking; Internet pedophilia; Internet pornography

Cyberassisted Online tax fraud; Physical assault with a computer (e.g., hitting someone over the head with a computer monitor); Property damage using a computer hardware device (e.g., throwing a CPU through a window)

7.3 Identity Theft

Cyberexcerbated; a crime in which an imposter obtains key pieces of personal information, such as social security or drivers license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.

7.4 Vigilante

Definition: a civilian or organization acting in a law enforcement capacity (or in the pursuit of self-perceived justice) without legal authority.

- Vigilantism reaction (often punishment) to real/perceived deviance.
- Involves planning and premeditation by those engaging in it
- Its participants are private citizens whose engagement is voluntary
- Form of autonomous citizenship that constitutes a social movement
- Uses or threatens the use of force
- Arises when established order is under threat from the transgression, potential transgression or imputed transgression of institutionalized norms
- Aims to control crime or other social infractions by offering reassurances (or guarantees) of security both to the participants and to others.

Internet technology facilitates the following:

- Allows the average person to play the role of the report/journalist to chronicle objectionable act (i.e. become reporters)
- Allows the average person to read/watch the footage of the act and take active actions in response (i.e. become vigilantes)
- Footage of the act could be easily circulated to a global audience
- Easier for the poster and the reader to remain anonymous
- Harder for the offenders to erase their label. The stigma may be permanent.

8 Big Data

8.1 Paradoxes

8.1.1 Transparency

Big data promises to use this data to make the world more transparent, but its collection is invisible, and its tools and techniques are opaque, shrouded by layers of physical, legal, and technical privacy by design. If big data spells the end of privacy, then why is the big data revolution occurring mostly in secret?

8.1.2 Identity

Big data seeks to identify, but it also threatens identity. This is the Identity Paradox. We instinctively desire sovereignty over our personal identity. Whereas the important right to privacy harkens from the right to be left alone, the right to identity originates from the right to free choice about who we are.

If we lack the power to individually say who I am, if filters and nudges and personalized recommendations undermine our intellectual choices, we will have become identified but lose our identities as we have defined and cherished them in the past.

8.1.3 Power

Big data will create winners and losers, and it is likely to benefit the institutions who wield its tools over the individuals being mined, analyzed, and sorted. Not knowing the appropriate legal or technical boundaries, each side is left guessing. Individuals succumb to denial while governments and corporations get away with what they can by default, until they are left reeling from scandal after shock of disclosure. The result is an uneasy, uncertain state of affairs that is not healthy for anyone and leaves individual rights eroded and our democracy diminished.

8.2 Privacy

- Companies and governments increase use of big data to improve products and services, including defending against terrorist and cybersecurity attacks
- Public increases questions about privacy and how data is used as realisation of invasions is brought to awareness

Privacy needs new focus. Instead of focusing on the collection of information, our new focus should be on the rules that govern how personal information is used and disclosed

- The rules that govern how information flows and not merely restrictions on acquiring personal information or data (Nissenbaum)
- But our practical ability to manage the trade of personal information needs to be fixed. How can we self-manage privacy?
  - notice: data processors should disclose what they are doing with personal data
  - choice: people should be able to opt-out of uses of their data that they dislike
- But is self-management a feasible route?

8.3 Confidentiality

Information exists in states between being completely private and completely public.

- Privacy is not binary. Important to recognise that.
- Before big data, individuals could more easily gauge the expected uses of their personal data and weigh the benefits and the costs at the time they provided their consent.
- For companies, the potential for harm due to unintended consequences, can quickly outweigh the value the big data innovation is intended to provide. Not limited to harm to individuals, but also institutions.
- Big data uses secondary information shared privately in confidence. Can we trust this information to remain confidential? How can it be regulated by law?

8.4 Transparency

The power of big data comes in large part from secondary uses of data sets to produce new predictions and inferences. Institutions like data brokers, often without our knowledge or consent, are collecting massive amounts of data about us they can use and share in secondary ways that we do not want or expect.

- Why is there privacy for institutions but none for individuals? How can this be better balanced? Those who collect, share, and use data must be made more transparent and thus more accountable.

8.5 Changes

Changes in law are essential but insufficient, usually slow. So how do we fill this gap?

- Chief Privacy Officers

- In-house philosophers (eg. Damon Horowitz at Google)
- Users (but requires institutions to be transparent)
- Technologists can fill these gaps by rebutting privacy is dead beliefs and moving to advance ethics of data, and creating new business models, practices and technologies
- Review boards (IRBs) for consumer experiments

9 Intellectual Property

9.1 Copyright

Copyright is a form of protection provided to the authors of original works of authorship including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly.

The copyright protects the form of expression rather than the subject matter of the writing. For example, a description of a machine could be copyrighted, but this would only prevent others from copying the description; it would not prevent others from writing a description of their own or from making and using the machine. Copyrights are registered by the Copyright Office of the Library of Congress.

9.2 Trademark

A trademark is a word, name, symbol or device which is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A servicemark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms trademark and mark are commonly used to refer to both trademarks and servicemarks.

Trademark rights may be used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark. Trademarks which are used in interstate or foreign commerce may be registered with the Patent and Trademark Office.

9.3 Patent

A patent for an invention is the grant of a property right to the inventor, issued by the Patent and Trademark Office. The term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. US patent grants are effective only within the US, US territories, and US possessions.

The right conferred by the patent grant is, in the language of the statute and of the grant itself, the right to exclude others from making, using, offering for sale, or selling the invention in the United States or importing the invention into the United States. What is granted is not the right to make, use, offer for sale, sell or import, but the right to exclude others from making, using, offering for sale, selling or importing the invention.

9.4 Labour Theory of Property

Locke argues that when a person mixes his or her labor with the land, that person is entitled to the fruit of his or her labor. So if a person tills and plants crops on a section of land that is not already owned by anotheran act which, Locke notes, requires considerable toilthat person has a right to claim ownership of the crops.

9.4.1 Criticisms

1. Intellectual Property are nonexclusionary in nature, and are thus not scarce
2. Property right is a natural right

9.5 Utilitarian Theory of Property

Property rights are better understood as artificial rights or conventions devised by the state to achieve certain practical ends. According to utilitarian theory, granting property rights will maximize the good for the greatest number of people in a given society. inventions. Incentives in the form of copyrights and patents would motivate individuals to bring out their creative products and that, as a result, American society in general would benefit.

9.6 Personality Theory

According to the personality theory of property, the intellectual object is an extension of the creators personality (i.e., the persons being, or soul). And it is because of this relationship between the intellectua object and the creators personality that advocates of the personality theory believe that creative works deserve legal protection.

10 Appendix

10.1 ACM Code of Ethics

10.1.1 Principle 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

10.1.2 Principle 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08. Accept no outside work detrimental to the work they perform for their primary employer.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

10.1.3 Principle 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.

3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05. Ensure an appropriate method is used for any project on which they work or propose to work.

3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07. Strive to fully understand the specifications for software on which they work.

3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users requirements and have the appropriate approvals.

3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

10.1.4 Principle 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01. Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

10.1.5 Principle 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance . In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with this Code.

5.12. Not punish anyone for expressing ethical concerns about a project.

10.1.6 Principle 6: PROFESSION

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

10.1.7 Principle 7: COLLEAGUES

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

10.1.8 Principle 8: SELF

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.