Should we trust automation? Can automation cause harm to individuals and to society? Can individuals apply automation to harm other individuals? The answers are yes; hence, ethical issues are deeply associated with automation. The purpose of this chapter is to provide some ethical background and guidance to automation professionals and students. Governmental action and economic factors are increasingly resulting in more global interactions and competition for jobs requiring lower-end skills as well as those that are higher-end endeavors such as research. Moreover, as the Internet continually eliminates geographic boundaries, the concept of doing business within a single country is giving way to companies and organizations focusing on serving and competing in international frameworks and a global marketplace. Coupled with the superfluous nature of an Internet-driven social culture, the globally-distributed digitalization of work, services and products, and the reorganization of work processes across many organizations have resulted in ethically challenging questions that are not just economically, or socially sensitive, but also highly culturally sensitive. Like the shifting of commodity manufacturing jobs in the late 1900s, standardization of information technology and engineering jobs have also accelerated the prospect of services and jobs more easily moved across the globe, thereby driving a need for innovation in design, and in the creation of higher-skill jobs. In this chapter, we review the fundamental concepts of ethics as it relates to automation, and then focus on the impacts of automation and their significance in both education and research.
47.1 Background

*To educate a man in mind and not in morals is to educate a menace to society.* (Theodore Roosevelt)

In this chapter we attempt to address a key issue facing people from industry and academia, especially with the rapid pace of globalization and technological advancement related to automation. Why is ethics, and what makes studying and understanding ethics and its link to automation important; both the inculcation of it among our present and future colleagues, employees, and public services, and understanding it within the context of academic, government, and corporate research. After describing the ethical issues related to automation, we focus our presentation on two specific areas, education and research, respectively. In the section on education, we present a mechanism whereby the inculcation of ethics can, and should, be integrated within a student’s curricular program and learning experience, instead of the simpler one-course approach that is taken by educational institutions today, in response to the mandatory requirement of teaching ethics as sought by employers and accreditation agencies such as ABET. The section on research could have been written on many levels – from ethics in workplace, personal ethics, to social and professional perspectives of what can be considered ethical behavior in research. Since these topics are widely covered elsewhere (references are given below), we have chosen to illustrate and explore the critically emerging issues of user profiling by logging user activities on a network (the Internet and automation networking in general). This illustration is important because this issue is beginning to assume a greater degree of significance in today’s world, with the ability of people and organizations to use advanced automation to gather, store, mine and analyze enormous amounts of data, very cheaply. Hence, addressing this issue will likely prompt ethical questions (not just limited to what we present here) across all the above different perspectives.

47.2 What Is Ethics, and How Is It Related to Automation?

*New and emerging automation technologies and solutions pose significant new challenges for ethical individuals, organizations, and policy-makers.* (Automation Scholars)

Ethics is a set of principles of right and wrong that individuals apply when making decisions influencing their behavior. Many decisions can clearly be recognized by most people as being wrong or immoral, including violations of the law, dishonesty, and any other behaviors that conflict with common behavioral norms and societal values. The role of ethics, ethical thinking, is important especially when there are no clear-cut guidelines, for example, when individuals encounter conflicts between objectives and their principles, and as often happens with the emergence of new technology, including automation technology [47.1–7]. As new choices and new experiences become available to individuals and organizations, they face dilemmas between risks and benefits, short-term benefits against long-term risks, risks to individuals versus benefits to a group, and so on. A major challenge to ethical behavior is the fact that not only changes in technological abilities over time pose new ethical dilemmas, but that ethics is deeply rooted in local and domain cultures, hence, it requires adjustments and calibration in the interfaces and exchanges. This dual challenge for inter-cultural ethical behavior over time and location has been evident throughout history, and is particularly sharp at the edges during our age of tremendous automation innovations coupled with intensifying global exchanges (Fig. 47.1).

Automation has several particular impacts on ethics:

1. Automation enables unethical behavior, e.g., applying automatic imaging to monitor private situations violates privacy rights, but may be necessary for security and prevention of theft.
2. Automation simplifies unethical behavior by obscuring its source, e.g., people blaming automation for mistakes, delays, inefficiency, and other weaknesses (*It’s not me; it’s this dumb computer*).
3. Automation increasingly enables unethical behavior related to information and communication, e.g., recording conversations and proprietary knowledge; maintaining and visiting web-sites with illegal, violent, or hateful contents.
4. Automation enables replacement of labor, e.g., by robots, automated sorting, and automatic inspection.
5. Automation affords anonymous access over and to private or restricted property.
Fig. 47.1a–d Ethics values and dilemmas: (a) Ethics of today may not be the same as ethics of yesteryears due to changes in cultural and technological evolution (changes) around the globe. (b) Ethical dilemmas are conflicts between individual’s or groups of individuals’ rights, benefits, and rewards versus community, organization, and society at large gains and sustainability. (c) Major ethical dilemmas emerge when changing from manual tools and procedures to automated and automatic devices, e.g., remote imaging, banking automation, and Internetworking. (d) Major ethical dilemmas further emerge, more frequently and with farther impact when automation evolves and with computers and worldwide network communications advancements.

6. Automation enables cyber-crime, cyber-terrorism, information hiding or obscuring, forgery, identity theft, or identity hiding. Some of these examples overlap with criminal and other illegal behavior [47.6, 8, 9]. But there are many examples where the situations are ambiguous, or ambivalent. When society realizes the severity and damage caused by some such cases, laws are developed and implemented. Often, however, ethical issues emerge and require urgent individual and organizational responses in the face of far-reaching ethical dilemmas.

47.3 Dimensions of Ethics

Dimensions of ethics can be considered in multiple aspects, which are inter-related (Table 47.1): From the aspect of automation technology, how and what it enables in challenging ethical behaviors, e.g., financial crimes through banking automation; from the aspect of impacts on individuals, on communities, and on society, e.g., hate crimes through the Internet. From the aspect of automation security, how automation’s own security can be breached with unethical schemes and outcomes, e.g., by intentionally or unintentionally disabling software safety functions. In all dimensions, however, it is clear that people are responsible, directly or indirectly, intentionally or unintentionally, for their ethical decisions, behaviors, and the outcomes; furthermore, people, not automation, are the potential misusers and abusers of automation in the context of ethics.

Ethics and automation can also generally be divided into ethical issues involving information-focused automation [47.1, 2, 4, 10], e.g., information security and privacy; and automatic device/systems ethic [47.7, 9, 11–13], e.g., ethics of robotics (sometimes called robotics), for instance, trust in tele-surgery by robots. There are, of course, overlapping ethical dimensions, for instance, when information systems are hacked (security breach) to disrupt automatic traffic and avation control (impact dimension), or to dysfunction automatic power distribution (technology and impact dimensions) [47.5, 14–16].
Consider the four main automation areas (Chap. 3, Fig. 3.2):

1. Automation with just computers – Data processing and decision support, e.g., enterprise resource planning, accounting services
2. Automation with various automation platforms and applications, but without robots, meaning automation with devices, sensors, and communication, e.g., weather forecasting, air-traffic control
3. Automation applying also robotics, e.g., fire safety including alarms and robotic sprinklers
4. Automation with robotics, e.g., robot painting, robotics in microelectronics fabrication and assembly

Each of these automation areas involves ethical decisions and behaviors, along the dimensions indicated in Table 47.1, by managers, operators, maintenance personnel, and designers, who have to adhere to ethical values to enable sustainable services and viable society. Additional examples follow below.

Another common view of ethics and automation has been the view from the aspect of impacts on individuals, on communities, and on society. Four main dimensions of ethics in this context, as related to automation, are privacy, property, quality, and accessibility.

Privacy: Privacy issues are related to gathering, maintaining, distributing, analyzing, and mining information about individuals. For example:

- What rights do individuals have to their own information and its protection?
- What information about themselves do individuals have to share with others?
- Who is responsible for the security of private information when it is maintained in a database?
- What rights to surveillance over individuals do organizations and government services have?

Property: Issues involving ownership of physical and intellectual property. For example:

- Can corporate automation equipment be used for personal purposes?
- How should software, music, and other media piracy be handled?
- Who is accountable and liable for damage caused by automation?
- How will intellectual property be traced and accounted for, when automation enables its easy and rapid copying and transfer?
- Who is responsible and accountable for backup records?

Quality: Quality of automation implies its integrity and safety of functions, fidelity, authenticity and accuracy. For example:

- Can an individual trust an automatic device, e.g., in medical diagnostics and treatment?
• What quality standards are needed to protect society's and individuals' safety and health, also including long-term environmental concerns?
• What quality standards and protocols concerning automation and information are required to protect individuals' rights?
• Who is responsible, accountable, and liable for the accuracy and authenticity of information and of automatic functions?
• Who is responsible, accountable, and liable when functions relying on automation fail?

Accessibility: Accessibility issues involve the right to access and benefit from automation, the authority of who can and cannot access certain automation assets and resources, and the increasing dependency on automation. For example:
• What skills and what values should be preserved and maintained in a society increasingly relying on automation?
• What about loss of judgment due to such reliance?
• Who is authorized to use automation and access automation resources?
• How can such access be managed and controlled?
• Can employees or clients with disabilities be provided with access to automation, for their work, healthcare, learning, and entertainment?
• How and under what conditions should access to automation be priced and charged?
• Can automation limit political freedom?
• Does automation cause addiction and isolation from family and community?

47.3.1 Automation Security

Automation security involves security of computer and controller software and hardware; of information and knowledge stored, maintained, and collected by automation, e.g., the Internet, imaging satellites, and sensor networks; and of automation devices, appliances, systems, networks, and other platforms. Most of the ethical concerns in automation security overlap the previous aspects and dimensions, but have certain unique security related dimensions. Some of the ethical issues associated with automation security are:
• What are the vulnerabilities of automation security that impact on privacy, property, quality, and accessibility ethical dimensions, and who is responsible for overcoming them? For recovering from them?
• With increasing automatic interconnections and automatic interactions between various automation systems and devices, how can security levels be maintained, shared, and warranted over entire services? Who is responsible for tracking, tracing, and blocking the instigators and initiators of the security shortcomings causing unsatisfactory service?
• Who is responsible and who is liable in the case of harmful and damaging security breaches, such as trespassing, espionage, sabotage, information extortion, data acquisition attacks, cyber-terrorism, cyber-crime, compromised intellectual property, private information theft, and so on? What would be the difference between breaches caused by unintentional human error versus malicious, unethical acts?
• Who is responsible and who is liable when there are automation software attacks, e.g., software viruses, worms, Trojan horses, denial of service, phishing, spamware, and spyware attacks?

Governments, national and international organizations, and companies have already advanced various measures of defenses and protection mechanisms against security breaches. Examples are the Business Software Alliance (www.bsa.org), the cyber consequences unit in the US Department of Homeland Security, computer and information security enterprises such as www.cybertrust.com, and university centers such as CERIAS (Center of Education and Research in Information Assurance and Security, www.cerias.purdue.edu), and CERT (Computer Emergency Response Team, www.cert.org). Yet, automation security poses complex and difficult challenges because of the high cost of preventing hazards, associated with the difficulty to justify such controls, the difficulty to protect automation networks that cross platforms, organizations, countries, and continents, and the rapid automation advances, which render new security measures obsolete. More about automation security can be found in [47.25–30].

The ethical dilemmas discussed above and their dimensions illustrate some of the ethical questions raised by developing and applying automation, and by its rapid advancement and influence over our society, from automatic control devices, robots and instruments, to the computing, information, communication, and Internet applications.
47.3.2 Ethics Case Studies

Ethics is best taught and explained through case studies and examples [47.2, 3, 5, 14, 21, 31, 32]. In Table 47.2, examples of ethical issues related to automation are described. Some examples are clear ethical dilemmas.

Table 47.2 Examples of ethical issues in automation and their dimensions

47.4 Ethical Analysis and Evaluation Steps

What is hateful to you, do not do to your fellow human. (Hillel the Elder, Talmud, Shabbat 31a)

How can one rationalize situations and decisions involving ethical conflicts? And how can automation systems be designed and operated with assurance that intended ethical imperatives and decisions would indeed be followed?

Some of the earliest thinking about ethics and automation, in the area of robotics, is attributed to Isaac Asimov, a prominent scientist and science fiction author, who wrote in his book *I, Robot* [47.33] and also in *Looking Ahead* [47.34] *The Three Laws of Robotics*:

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

Substituting an automation system for a robot in the three laws above would still make a lot of sense in any context of automation, including the threat of automation singularity (see Chap. 3). But a critical issue is how to implement it during the design and activation of any automation functions. While this challenge is still open to research and discoveries, ethics educators and scholars recommend a five-step approach, as follows [47.1–8, 18, 19]:

Step 1 Characterize and Specify the Facts
Establish the stakeholders and events involved, including the 6 Ws; who, what, when, why, to whom, and where.

Notes:

a) Sometimes, just clarifying the facts results in simplifying the resolution and the decision.
b) Often getting multiple parties, even those in conflict, to agree on the facts may help resolve the ethical conflict.

c) Often the clarification of facts sharpens and simplifies the realization of an ethical imperative, leading one or more of the participants to share the facts with authorities (known as the whistle blower), thus leading to a resolution of the ethical dilemma.

Step 2 Formulate the Dilemma and Conflict (or Conflicts), and Find the Involved Values
Ethical issues are always linked with values; the parties in conflict usually claim their motivation as the pursuit of high values, such as fairness, freedom, protection of privacy and property, saving resources and the environment, and increasing quality.

Step 3 Clarify Who Would Benefit and Who Would Be Harmed by the Given Ethical Issue
Beyond the facts established in Step 1, including the stakeholders, analyzing and finding who may benefit and who may be harmed can be useful in clarifying and understanding which solution, or solutions, may be effective and feasible and practicable.

Step 4 Weigh and Balance the Resolution Options
Ethical dilemmas and conflicts are characterized by having complex variables and dependencies, and rarely present a simple solution. Usually, not every one of the stakeholders and other involved individuals, organizations, and society members can be satisfied. Moreover, the thorny realization is that there would almost always be some who may suffer or would consider themselves harmed under any given decision. In some cases, there may not be any optional strategies that could balance the consequences to all the involved parties.

Step 5 Analyze and Clarify the Potential Outcome of the Ethical Decision
Certain options of ethical strategy and policy to resolve a given ethical dilemma may satisfy our principles and values, yet they may be harmful from other aspects. For example, a policy
### Ethical case

<table>
<thead>
<tr>
<th>Dimension of ethical issues</th>
<th>Privacy</th>
<th>Property</th>
<th>Quality</th>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Company database highlights employees’ personal attributes,</strong> e.g., nearing retirement, potentially being discriminatory. Furthermore, who needs to know this information? Who is authorized to access it?</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>2. Service providers monitor employees’ access to certain websites.</strong> Employees cannot prevent being monitored while using company computers; employers may abuse the gathered private information.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>3. Organization audits individuals’ use of unauthorized software,</strong> either to create policies, protect itself from property lawsuits, or monitor individual private behavior.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4. Company is using automated imaging technology to replace employees.</strong> This case illustrates a typical conflict between economy, accuracy, and efficiency goals achievable with automation, and the loyalty to dedicated employees (who will lose access to work with automation).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>5. New automatic sorter has hidden design deficiencies that are too costly to repair after deployment of thousands of such devices.</strong> This case is common, as evident by some ethical companies occasionally recalling defective automation equipment for upgrade and repair. If there is no recall in such cases, clients and users are denied access to better quality and safer equipment.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>6. A robot controller, under certain undisclosed conditions, will cause substantial chemical waste and pollution.</strong> This multi-dimensional ethical problem, involving issues of significant potential damages to life, life quality and property, possibly denying access to inflicted areas and properties, and potentially costing also in major remedial and recovery efforts, is illustrated by cases of whistle blowers, ethical individuals who risked their employment to warn about imminent hazards.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>7. Company has superior medical automation technology but will not produce it for several years till it recovers all previous investments in the inferior product currently being marketed to hospitals.</strong> This case is similar to Case 6, except it is a different scenario.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>8. A vending machine delivers (a) the right item, but returns too much change; (b) the wrong item, and no change.</strong> Ethical dilemmas are caused by automation’s dysfunctional quality.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>9. A manager blames automation for faulty packaging.</strong> Is automation to blame, or is it its designer/implementer/user?</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10. A student blames the school’s computer for lost homework.</strong> Ethical challenges concerning work quality (and computer automation quality) are posed to both the student and the instructor.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11. (Think of an ethical dilemma with your home automation.)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>12. (Think of an ethical dilemma unique to your organization’s use of automation.)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 47.3: Examples of conflicts between ethical values and principles

<table>
<thead>
<tr>
<th>Values/Principles in conflict</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Short versus long term</td>
<td>Software patch solving security problems now but causing hazards later</td>
</tr>
<tr>
<td>2. Individual versus community</td>
<td>Wasteful exploitation of resources harming later generations</td>
</tr>
<tr>
<td>3. Justice versus mercy</td>
<td>Charging for mass email to prevent spamming</td>
</tr>
<tr>
<td>4. Privacy versus convenience</td>
<td>Reading the fine details of use-contracts for each downloaded software</td>
</tr>
<tr>
<td>5. Loyalty versus truth</td>
<td>Divulging harmful private or proprietary information gained in confidence</td>
</tr>
<tr>
<td>6. Loyalty to present</td>
<td>Sharing knowledge about relative advantages or shortcomings of design</td>
</tr>
<tr>
<td>versus former organization</td>
<td>(employer)</td>
</tr>
<tr>
<td>7. Efficiency versus safety</td>
<td>Higher speed limits and lower weight versus automobile accidents’ severity</td>
</tr>
</tbody>
</table>

In analyzing ethical conflicts, usually the conflicts between two or more right solutions, or between two or more right values, pose the most complicated dilemmas. For example, decisions in examples 1 and 5, which may be relatively simple when the potential hazard is enormous. The situations are also relatively more complex when multiple conflicts combine, e.g., individual versus community for short versus long term implications. Additional guidance is offered by ethics principles.

### 47.4.1 Ethics Principles

Numerous ethics principles have evolved since ancient times, and have been suggested by ethics philosophers and scholars. Seven of the well known principles are listed in Table 47.4.

Principles (1) and (2) are considered the *individual fairness* principles. Principle (3) is similar to (2), but stated from a group aspect. Principle (4) represents the

<table>
<thead>
<tr>
<th>Principle’s name</th>
<th>Ethical principle imperative/lesson</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hillel the Elder’s principle</td>
<td>Do not do to others what you do not want to be done to you.</td>
</tr>
<tr>
<td>2. The Golden rule</td>
<td>Do to others what you would accept if done to you.</td>
</tr>
<tr>
<td>3. Immanuel Kant’s categorical imperative</td>
<td>If an action is not right for everyone (in a team, group, or community) to take, then it is not right for anyone.</td>
</tr>
<tr>
<td>4. Descartes’ rule of change</td>
<td>If an action cannot be taken repeatedly (e.g., a small action that may snowball out of control), it is wrong to take it at any time.</td>
</tr>
<tr>
<td>5. Utilitarian principle</td>
<td>Decide on the action that leads to the higher, or greater, or more significant value (if values can be prioritized, and if consequences can be predicted).</td>
</tr>
<tr>
<td>6. Risk aversion principle</td>
<td>Decide on the action that leads to the least damage, or the smallest hazard.</td>
</tr>
<tr>
<td>7. No Free Lunch rule</td>
<td>Respect the ownership of tangible and intangible assets, and if ownership is unknown to you, assume somebody owns assets that do not belong to you.</td>
</tr>
</tbody>
</table>
impact of time and changes over time (at least those changes that are predictable. Principle (5) addresses the issue of conflict between several objectives and principles, and maximizing the value of consequences. Principle (6) is similar to (5) but from the aspect of minimizing damage. Finally, principle (7) addresses the value and concern for intellectual property protection, on par with physical property protection, as a fair principle for a globally sustainable society.

The above principles provide some guidance for initial analysis. Often, however, they may point to conflicting strategies, and individuals still need to carefully weigh their decisions and take responsibility for each of their decisions. On the other hand, these basic principles offer clear tests for actions and decisions that should not be followed if they fail these tests.

47.4.2 Codes of Ethics

To address the complexities of ethical issues, corporations and organizations define, accept, and publicize their code of ethics [47.10, 21–23]. Such a code prescribes values to which the organization or corporation members are supposed to adhere. The typical structure of a code of ethics closely related to automation is illustrated in the Appendix. Examples of codes of ethics in different countries are included on the USA National Academy of Engineering site ([47.21], http://onlineethics.org). Values that may be incorporated in a code of ethics include:

- Care for others
- Compliance with the law
- Consideration of cultural differences
- Courtesy
- Fairness
- Honesty
- Integrity
- Loyalty
- Reliability
- Respect for sustainable environment
- Trustworthiness
- Waste avoidance and elimination.

General moral imperatives that are included in a code of ethics are listed as follows:

- Follow fairness principles
- Contribute to society and human well-being and sustainability
- Avoid harming others
- Be honest and trustworthy
- Honor property rights including copyrights and patents
- Give proper credit to intellectual property
- Access automation resources only when authorized
- Respect the privacy, diversity, and rights of others.

47.5 Ethics and STEM Education

I didn’t know I was a slave until I found out I couldn’t do the things I wanted. (Frederick Douglass)

Rapid advancements in automation have led to significant challenges, as indicated earlier in this chapter. Automation has also influenced changes to demographics, and the creeping of problems associated with student and employee recruitment, retention, and focused funding. Good educational preparation in the science, technology, engineering, and mathematics (STEM) disciplines is one of the primary means available to prepare the workforce to compete globally for highly skilled technology-based and automation-based jobs. In their current work environments, not only do students need to understand and deal with the increased knowledge expectations from the workforce, but they need to also understand and deal with the pervasive and dominant role of automation technology within their chosen fields, and operate effectively in an increasingly multi-cultural and multi-ethnic, global environment. In these jobs, softer skills, which relate to how we go about getting things done, being language, society, and culture-sensitive, are becoming equally important as the hard functional skills (e.g., programming, problem solving, techniques selection, modeling) that have traditionally defined what it means to be competent in a chosen professional field. The widespread globalization of the job market calls for future employees to be adaptive, curious, and nurturing so as to work effectively in a team, which may be either co-located or geographically separated.
47.5.1 Preparing the Future Workforce and Service-Force

_“I cannot tell anybody anything; I can only make them think.” (Socrates)_

Many organizations, for profit and not-for-profit, now realize that hiring workers who have been trained to understand international issues, specifically from an ethical and cultural perspective, will provide their businesses and services the necessary competitive-sustainable advantage in a global society and global market. For example, conducting transactions in another country can be riddled with cultural issues that require deft personal touch, such as demonstrating appropriate hospitality, and respecting cultural and religious diversity. Thus, the future in many professional disciplines is not in merely a collective ability to prepare and graduate good designers, programmers, practitioners, managers, and technologists – these skills have now become commodities that can be outsourced. It lies in the ability to prepare entry-level employees and continuing education employees who are highly comfortable with the theory, can appropriately blend it with necessary practice and possess an understanding of both the business culture and the social issues involved, while being able to effectively share, communicate, articulate, and advance their ideas for an innovative product or solution. Hence, how we educate students to become such successful employees and entrepreneurs, while acting ethically in the global economy and society is an important consideration, often better taught through the use of appropriate case studies.

The rapidly emerging and evolving, and highly sensitive global economy is profoundly affecting the employment patterns and the professional lives of graduates. Thus educating the future workforce to understand such issues in a global context is becoming a highly sought-after experience and a critical differentiator in their employability, often testing their ability to bridge discipline-specific theoretical research issues with real-world practice, including addressing and resolving ethical dilemmas, as reflected by the inundation of single and multi-semester capstone projects in many disciplines. While it has been widely reported that despite intensifying competition, off shoring between developed and developing countries can benefit both parties, many students from western countries have shunned STEM careers because they fear that job opportunities and salaries in these fields will decline. Thus, education is confronted with needing to provide students with higher-order technological skills aptly blended with the consideration of emerging social needs across the globe to provide much needed experiences to thrive in the future, as well as be frontline contributors to the technologically and ethically savvy workforce.

A fundamental change in the education of future workforce and service-force is necessary to assure that we are well prepared for the increasingly more professionally demanding roles. These demands relate to success in the job market, responsibilities toward employers, customers, clients, community and society, and responsibilities as developers of powerful and pervasive automation technologies. In addition to strong technical and management skills, future software and automation designers need the skills to design customized products and integrated services that meet the diverse needs of a multi-cultural, multi-ethnic, and increasingly smaller world united by rapid scientific and technological advances, and facing globally and tightly inter-related hazards and challenges. These trends come with unforeseen social and ethical challenges and tremendous opportunities.

47.5.2 Integrating Social Responsibility and Sensitivity into Education

Effectively integrating social-responsibility, sensitivity and sustainability into our educational curricula has become essential for employers and organization leaders [47.32, 35–37]. See also, for example, the IEEE and ACM model curricula in the context of automation (IEEE.org, ACM.org). Students, trainees, and employees need the diverse exposure to problems and ideas to develop a broad, yet pragmatic vision of the technologically-shifting employment and business landscape. A case study-based approach to teaching, training, and inculcating ethical behavior can provide adequate opportunities to develop the necessary soft skills for being successful in the global service and workplace. Such an exposure can vastly benefit those who may very well be charged with developing policies, priorities, and making investments that can help regions and nations to remain competitive and integrated in the global automation systems and services industry.

Many STEM curricula, in response to these growing industry needs, have placed emphasis on team-based projects and problem-based instruction styles. However, these projects have their own bag of pit falls; for example, in project-based software development classes students often epitomize software development as building the best solution to address customers’ re-
requirements. In the following section, a dilemma-based case study approach that goes beyond a project-based curriculum is described. It encourages students to reflect upon the social and ethical ramifications of technology, expanding the narrow, functional-focused tunnel vision that currently (subliminally) exists across many computing and automation curricula, and the automation and software industry, in particular. This is an attempt to address some specific concerns that arise out of such a problem/project focused curricula. With respect to automation and software-related issues, some of these concerns include:

1. In today’s post-scandal business climate, additional scrutiny, public condemnation, and possible legal consequences could result if individuals and companies continue to violate accepted ethics and fairness standards. While it is often difficult, if not impossible to predict the future, or the negative consequences of a creation, is ignoring such possible consequences on individuals not ethically questionable?
2. Is it responsible automation development practice, when creating a new technology, and is it ethically sound enough with regard to any possible negative consequences of the new creation and its effects on society?

### 47.5.3 Dilemma-Based Learning

> Education is what remains after one has forgotten what one has learned in school. (John Dryden)

**Case-based learning** has long been used in management and business schools [47.38, 39]. It has also proved to be highly effective in other disciplines [47.40–42]. According to [47.43], “Students change profoundly in their ability to undertake critical analysis and discuss issues intelligently”. Case-based instruction offers a number of advantages and is effective for increasing student motivation [47.40, 41]. In summary, it is thought to be more effective than didactic teaching methods because real-world cases:

1. More accurately represent the complexity and ambiguity of problems
2. Provide a framework for making explicit the problem-solving processes of both novices and experts
3. Provide a means for helping students develop the kind of problem-solving strategies that practicing professionals need [47.44].

**Problem-based learning**, a case-based derivative, is also widely used, where students are required to learn and apply assimilated knowledge [47.45]. It is reported to broaden students’ views and causes a new awareness of their own ideologies and capabilities, and effects growth, questioning, or affirmation [47.42].

In **dilemma-based learning** [47.31, 37], another case-based derivative, a story or game is used to communicate the feeling of real-life dilemmas, while challenging its users to learn from the results of their actions. Dilemmas are chosen for their relevancy to complex and costly situations that are difficult for people to comprehend. For example, dilemmas may reflect the complexities of network implementations or the impact of blame on team productivity and project costs. Dilemmas in the classroom challenge learners to balance trade-offs between short-term rewards and long-term results [47.37]. In prior work, it has been noticed that discussions on real-world topics through dilemma-based case studies that couple logical investigative thinking of the problem-based approaches with strategic needs assessments – cost, performance metrics, etc., make appropriate sense in motivating CS students [47.32, 35, 37].

The use of enthusiasm, empathy, and role-play by students has also been shown to be beneficial in improving overall student attitude and encouraging more participation by women students and minorities [47.36, 46]. It helps develop learning communities and other forms of peer support structures, while emphasizing the positive social benefits of automation and computing. It instills a good feeling among students and motivates them to be participative [47.47, 48]. Hence, a secondary effect of this approach is to help student retention efforts, as they explore related technology issues and interests in the various domains based upon their own personal analogical contexts and experiences. Thus, a recurring dilemma-based approach integrated into multiple automation and computing classes could help increase retention of acceptable ethical standards among students regarding automation technology and help them better understand different ethical issues and perspectives.

Dilemma-based learning, by adopting and building upon themes that dominate our everyday lives, in introductory level classes can not only have the greatest impact on subsequent classes, but also help correct the bad blame-driven rapport that the engineering and computing disciplines have received since the 2001 market crash. Progressive refinement of knowledge gained through more dilemma-based cases in different
classes throughout the curriculum provide the natural progression necessary for the retention of ethical issues, while allowing for reinforcement learning through similar dilemmas, but with increasing technical content of cases.

Currently, for interested educators, there are several archival case resources (this is a partial set of references to such material) on ethics with appropriate real-world cases that can be adapted to the needs of a particular class (e.g., [47.1–7, 21, 50, 51]). They can serve as resources to start the building of dilemma-based case studies across several core classes in automation-related curricula.

47.5.4 Model-Based Approach to Teaching Ethics and Automation (Learning)

Several model-based approaches to teaching ethics and automation have been developed and implemented effectively. For example, in [47.21] a model for teaching information assurance ethics is presented. The model is composed of four dimensions:

1. The moral development dimension
2. The ethical dimension
3. The security dimension
4. The solutions dimension.

The ethical dimension explores the ethical ramifications of a topic from a variety of perspectives. The security dimension includes ways in which an information assurance topic manifests to information assurance professionals. The solutions dimension focuses on remedies that individuals, groups of individuals, and society have created to address security problems and associated ethical dilemmas. The moral development dimension describes the stages and transitions that humans experience as they develop morally, and as they develop their own personal beliefs and behaviors about right and wrong.

Another model-based approach [47.49] is the IDEA model, described next.

The IDEA model presents how dilemma-based learning can be accomplished. There are two primary players and four steps to the IDEA model (Fig. 47.2). The players include the teachers involved in teaching the courses and the participating students. The four steps are, in turn, specific to these players. The four steps are explained in more detail and illustrated next.

**IDEA Step 1: Involve and Identify**

From the teacher’s perspective, the ‘I’ in IDEA stands for involve and from the students’ perspective it stands for identify. The teacher begins by engaging in a discussion of specific cases that are related to the topic being discussed in the class. For example, in an introductory programming course the discussion may be based on a case that is related to the issue of outsourcing. The teacher presents various concerns with respect to the case in question while at the same time engaging the students’ interest through discussions (several societal...
issues can be discussed here: job loss, immigration issues, changing business culture, companies relocating to other countries, etc.

By engaging the students in the identification of appropriately interesting cases, they become active participants in the class discussions and hence are more likely to engage in investigating the case study further from various socially-interesting perspectives.

A case study on outsourcing provides the ideal opportunity to dispel some of the pervasive myths that students seem to be swayed by, in their choice of automation and computing as a career choice. Current world news information is critical to involving students in the topic of discussion.

For example, at the time of writing this chapter, in the current state of the economy (August 2008), according to the CIO magazine, the unemployment rate for people in the IT industry is less than 3%, while that for the entire USA is 5.9%. Such information opens up the classroom for engaging discussions on IT-driven outsourcing myths and realities. In the rest of this section, we use outsourcing as an engaging example to illustrate the IDEA model. However, this example is by no means meant to be restrictive; other relevant examples may be issues of poor GUI design, issues with electronic voting machines (especially in years of national elections), issues of multi-language support in browsers, issues of robots in tele-surgery, issues with automation for earthquake rescue and refugee survival, automation innovations for energy production, distribution, and delivery, etc.

IDEA Step 2: Direct and Develop
In step 2, most possibly in a follow up class, the student is directed (guided) by the teacher to explore some specific issues of the case further to develop a deeper understanding of the various issues involved. Following the outsourcing case study identified earlier, say an automation assembly language programming class, students can be engaged in a discussion of software outsourcing for embedded systems, say the development of software modules such as drivers that are further integrated into everyday automation systems. Issues of security and privacy that are affected by these low-level software modules, which may be produced in any part of the world, can be discussed and articulated. It has been observed that students participate in such engaging topics with great enthusiasm. This enthusiasm allows learners and trainees to develop a mental model of the entire issue, as well as understand some of the subtle issues in the globalized system of automation software development, as well as appreciate the finer details of even studying a subject such as assembly language programming and its need within an automation and computing-based curriculum.

Often, students tend to develop a follow the herd mentality and are swayed by what they see and hear as requisite job skills. Students may often espouse the clouded view that they need to spend most of their time in the program learning marketable skills – such as the next hot programming language or system. By association, they may believe they should not spend time learning issues that may not be directly related to their immediate future jobs. This learning misconception has indeed been the observation of instructors and trainers in many disciplines.

Hence, although highly relevant to learning the fundamentals of automation, or computer science, courses such as assembly language programming, evoke less interest among current-day students. Integrating such a dilemma-oriented case study driven discussion can help assure the students of the need for focusing on such fundamental courses as well as understanding its high relevance to societal needs – for example, helping build privacy and security in I/O drivers and embedded automation devices and systems.

IDEA Step 3: Evolve and Explain

The mediocre teacher tells. The good teacher explains. The superior teacher demonstrates. The great teacher inspires. (William Ward)

In step 3, the ‘E’ in IDEA stands for evolve from the teacher’s perspective, and explain from the students’ perspective. The student, in the same (automation programming/digital design/assembly language) or a follow up class (say a database systems class that normally appears in a junior/senior year of the curriculum) is guided by the teacher to explore more details of the case to understand the magnitude and implications of the various issues involved. Again, on the issue of outsourcing, the teacher can engage the students in cases such as credit card sales and marketing (or cellular communication devices, etc.), whereby the jobs of identifying and seeking likely customers are outsourced to BPO companies (business process outsourcing).

Foreign governments are offering significant fiscal and non-fiscal incentives to attract such foreign direct investments into their respective countries and hence it is difficult for a business to ignore such compelling benefits. Experts who see the growing global demand for BPO (estimated to be at US$180 billion in 2010) indi-
cate a shift from cost-effectiveness to issues of skills, quality, and competence. Issues of personal, professional, and business ethics would definitely be factored as we move towards meeting such expectations, often driven by concerned citizens whose personal data is at stake as part of such BPO decision processes in multinational organizations.

In a course such as database systems, the teacher can guide discussion on how such practices effect the compilation, sharing, and administration of the data contained in large-scale distributed databases in question, their effect on issues of an individual’s privacy, which possibly is no longer within the geographical confines of the source country, and issues of checks and bounds verifications that need to occur for such business arrangements between business operating in across different countries that are culturally different.

How is an individual’s right to privacy different across cultures and what does privacy mean in a different society? What are the issues a business needs, or service needs, to be concerned with respect to the laws of the country? How can the business or service contain and secure the assimilation and sharing of such data? Instructors can promote discussions that can actually engage the student in understanding core values that may be viewed differently across cultures and grow by discussing cases that involve such experiences.

**47.6 Ethics and Research**

Collectively this book provides a wealth of automation-related research topics: sensor networks, cybernetics, communication, automatic control, soft computing, artificial intelligence, evolutionary automation, etc. All these automation research topics may serve as valid, timely topics for ethical concerns related to research; highly appropriate for this section. For the purposes of demonstration of emerging issues that can be ethically-sensitive vis-à-vis research, we focus specifically on the ethical issues related to research aided by the exponential growth of the World Wide Web and the information it could offer research about Internet users [47.52].

In order to advance research and serve the users of their products, many Internet companies keep web access logs, search history logs, or transaction logs. Why is this perspective of logs important? On bulletin boards, peer-to-peer and social networks, e-Commerce sites, and the Internet in general, individuals can behave and operate with certain anonymity in the absence of the presentation of self. Individuals online have a sense of complete autonomy and anonymity. Often the learnt social norm from such interactions is that there is little incentive to feel responsible for one’s own actions or sensitivity to the open public and community, in general, if the community does not provide some kind of instantaneous visible reward or tangible penalty.

**47.6.1 Internet-Based Research**

The scaling up of web content as well as users has resulted in increased difficulty in searching for information over the web. The ever increasing number of pages that match any given set of query words compel users to modify their queries a number of times before obtaining the required information. This repeated, inefficient search results in increased traffic on the network and in a spiraling effect, which in turn results in higher resource consumption and overload. Search engines have
made it possible for anyone to look up information from any corner of the world on the Internet.

In an unprecedented decision statement a judge in New Zealand banned online media from publishing the names of two people accused of murder [47.53]. All other news media such as TV, printed media, etc. were allowed to publish the names except the Internet media. This distinction was based on the concern that information about the accused is available on Internet for a long time even after the trial is over.

This case poses a dilemma about the information available on the Internet and in search engine logs much longer after the validity of the information has expired. The availability of query log datasets such as AOL has opened up the doors for carrying out exploratory research on searching user query logs and coming up with possible solutions to make the user search sessions more productive with the intent to provide better search experience for users. While AOL seems to have not taken adequate measures to hide personally identifiable information, the availability of the data set itself poses interesting ethical questions.

Several related developments can be summarized about research and internet-based search, which may shed light on ethical concerns and conflicts in this domain:

- In order to encourage research with user search query logs, Microsoft announced that it would avail its dataset to selected research organizations upon signing agreements. Such safeguards are necessary to protect user privacy and advance research, while developing better tools to help search engine users. Users’ opt-in and opt-out, meaning personally selective, optional acceptance or rejection of sharing their personal information, have become common as part of codes of privacy [47.4].
- Users’ web searching behavior has been an interesting research area for some time now. Researchers have studied the overall nature of information behavior, including information seeking behavior [47.54], information retrieval (IR) with hidden behavioral patterns and semantically superconcepts [47.55,56]. Sometimes, the thirst for information and convenience influence human searchers (as well as purchasers on the web researching available options) to willingly compromise, at least in part, their principled sensitivity to protect their privacy.
- Privacy rights and protection privileges are also associated with the availability of user search query log datasets. Included are multi-faceted logs coupled with relevant information such as time spent on the web page clicked on, web pages opened, printed and/or bookmarked, and whether the user’s true or at least intended information needs are satisfied. Potential ramifications or lack of such query logs dataset vis-à-vis user privacy issues are outlined in [47.57–59] and are subject to further research.

Addressing privacy rights and issues and Internet-based research requires review boards, as described also in the next section. Ethical thinking in this direction includes, for example:

- Setting up a review board for release of query log data for research purposes, while adhering to certain guidelines of ethical practices [47.60].
- Classifying sensitive queries in the query log dataset from a privacy perspective; for example, by partial anonymization of queries [47.61].
- Specific methods of anonymizing sensitive queries in the AOL and similar such datasets [47.62, 63]. For instance:
  - applying threshold cryptography systems that eliminate highly identifying queries in real time, and
  - dealing with a set of aggregated queries that are overly identifying, and addressing issues of tradeoff between privacy and utility of the query log data.

### 47.6.2 More on Research Ethics and User Privacy Issues

While internet users’ search session data availability for research and other exploitation illustrates serious ethical issues, some of which are described above, other privacy, property, quality, and accessibility ethical concerns need to be addressed. These concerns need to be appropriately handled, including: fair use of information, ethics of anonymity, and critical need for carefully enabling selective access to private information and behavioral research for specific goals of information for safety, health, security, and other essential public needs [47.64].

#### Privacy and Accessibility Rights

**Versus Significant Public Service**

What about limiting research on behavior patterns, which may result in losing the opportunity to obtain unique results for targeted services that are significantly beneficial to society, even critical for sustainability? For
example, health, safety, and security related issues may need Internet-based and mobile phone-based research. An emerging optional way is to have informed consent from the users at appropriate instances, to enable the fair use of behavior information for agreed upon and selectively chosen research activities. This area is being addressed already by different industry segments and is handled by various legal means.

Policies for Conducting Research Based on Automation
Policies for research based on knowledge obtained by automation have been developed and are still emerging to address ethical concerns, e.g., [47.65]. Initiatives have emerged and need to be strengthened and widened to satisfy World Wide Web media related issues, as such data may become increasingly available for organizations to mine for gaining competitive advantage in the market place, e.g., [47.33]. A consortium for university researchers, industries, government agencies, and other concerned organizations to discuss policy and other related issues of conducting such research is being developed.

The Myth About User Privacy with Automation
One myth about privacy of automation-users is that protecting privacy rights is the onus of the user. In today’s world, where information systems security management is a discipline that is fast emerging, its peripheries are yet to be well defined. Who are the gatekeepers?

- Internet service provider (ISP) are burdened with the responsibility of being gatekeepers of their users’ privacy; they have to regularly compromise with governmental agencies trying to gain access to ISP user data in order to prevent crime or conduct data forensics.
- Search engine services have a similar responsibility, though they are not burdened with the bulk of keeping the identity of their users private (exceptions being Google or Yahoo! users who may opt to log in before conducting a web-based search).

Neither of these entities, the ISP and the search engine service, would like to be burdened with the bulk of the responsibility of protecting the identity of a user, when the user performs web-based searches. But the fact is that the necessary interface for Internet access is provided to the user by the ISP. This fact lays the primary responsibility of user identity obfuscation squarely on the ISP. ISP employees may be able to gain access to searches conducted by their users and may be able to exploit these details in various unethical or ethical ways. This risk is higher in smaller communities that have populations less than 50,000 and are typically serviced by a few local ISPs.

Policies on Data Mining for Efficiency
Automation data preservation, analysis and indexing are important for web-based search engines and other Internet companies and automation services to perform efficiently, since correlating diverse user searches and interactions are the modus operandi of enhancing performance results. This information can be useful for automation design and architecture evolution. However, this data mining can also be misused by the automation service provider. Self regulations should be supported by clearly defined policies on how the data is collected, accessed, and distributed even for research purposes.

Institutional Review Boards
As common with any research involving human subject, universities and research organizations need to follow strict review board scrutiny. The Internet data research initiatives undertaken by universities and research organizations should also go through institutional review boards’ (IRB) formal approval process to make sure human interests, rights, and privacy are protected. Since the review, scrutiny and approval procedures can also be automated, Internet service providers and companies should set clearly defined guidelines and policies for its researchers and users. Many companies already focus on establishing a working group of individuals from privacy, legal, IRB, and security teams to discuss various aspects of the problem and proposed solutions. Such working groups study problems on a case by case basis ensuring a company’s competitive advantage without compromising on the ethical issues (if any) involved in the research.

The ethical issues about research and automation will undoubtedly be addressed as organizations and society learn the pitfalls and find methods to resolve the ethical dilemmas that have been mentioned. At the same time, it is clear (as indicated in Fig. 47.1) that newly developed and far reaching automation functions will continue to pose tremendous ethical challenges to individuals, organizations, and society at large.
47.7 Challenges and Emerging Trends

In this chapter, ethical challenges, dilemmas, and conflicts related to automation and enabled or introduced by automation have been highlighted. The context of automation and internationalization, or globalization of services and businesses bring further need for rational, acceptable, and sustainable ethical sensitivities and behaviors. These should continue to be the responsibility of individuals, and of individuals within organizations, but should also be supported, monitored, and maintained by automation mechanisms. Therefore, the increasing attention being paid to ethics in the context of automation, specifically from the perspective of education and research, has been explained. Challenging ethical issues have been presented and illustrated relative to the dimensions of technology, security, privacy, property, quality, and accessibility.

For education and training, the model-based approach for integrating ethics and socially responsible automation/computing into the undergraduate curricula, as well as training courses, has been presented. Examples from automation and computing curricular perspective have been used, and can be adapted to other science and technological disciplines, and commercial and service organizations. For the effective application of this approach, or similar programs, one needs the participation of several multi-disciplinary members, instructors or trainers. However, the attractiveness of such an approach is in its ability to engage the students and trainees meaningfully while still undertaking the primary task of learning the skills and techniques they would need to be successful upon graduation or completion.

For research, certain open challenges in gathering, mining, and observing user information-seeking behavior, while maintaining individuals’ privacy rights have been heightened. Policies, including review boards, have been and are being developed to address these ethical concerns. In such situations a strong rational balance between advanced research and user privacy must be maintained at all times. While the research community at large would come up with the solutions, privacy, anonymity, and fair use issues need to be effectively addressed to demonstrate the innumerable benefits that such research work can yield for the great benefits of individuals and of society. Marketing and information dissemination in a digital world represent an emerging area of research that can be timely and exciting for students, for users, for organizations, and for the public – for example, issues such as cookies leaving digital trail mixes on people’s machines, in light of protecting society, while also protecting individual freedom and individual rights.

47.7.1 Trends and Challenges

Ethical issues, dilemmas, and conflicts, and unethical behaviors, some of which are horrendous and tragic, are unfortunately an integral part of the proliferation of computers and automation in our lives. Major concerns range from privacy, copyrights, and cyber crime issues, to the global impact of computers and communication, online communities and social networks, and effects of virtual reality. Articles, books, conferences, on-line resources, social and political processes have evolved and continue to grow in importance and influence, contributing to ethics expertise in diverse disciplines. The breadth of multi-disciplinary scope allows students and professionals to learn, understand, and evaluate the individual, social, and ethical issues brought about by computer and automation technologies.

Some specific trends to consider:

International Policies
Impact of digitized information on individuals, communities, organizations, and societies, including continued discussions and necessary development of international policies on:
- Privacy
- Automation quality and reliability
- Automation security
- Copyrights and intellectual property
- Collaborative protocols for rational automation control, equality of access under authorization procedures, and trust and authentication agreements

Frameworks and Regulations
Development of ethical frameworks and regulatory processes are needed for substantial treatment of the interrelated automation issues of cyber-ethics: accessibility, free speech and expression, property, privacy, and security.

Self-Repair and Self-Recovery
Research and development of automatic self-repair and self-recovery are needed to address the risks as-
associated with unexpected computer and automation break-downs, disasters, and failures that open up vulnerabilities to unethical, unsustainable scenarios.

**Ethical Automation**

Research and development are needed of *inherently* ethical software and ethical automation (including ethical robotics) able to automatically handle and automatically help resolve issues such as media copying, file sharing, infringement of intellectual property, security risks and threats, Internet-based crime, automation-assisted forgery, identity theft, unethical employee surveillance, individual privacy, and compliance with ethical and professional codes.

**Ethics of Robotic Automation**

Major advancements are needed in robo-ethics to address the fact that (1) robots and robotic automation are increasingly more capable, and (2) there are humans that will increasingly abuse these powerful capabilities, deploying them in ethically questionable situations and environments (e.g., in schools, hospitals, etc.) where ethically wrong robotic automation conduct could have disastrous impacts on humans.

- We must develop ways to ensure that automation, without robots and with robots, will always behave in an ethically correct manner.
- We need to be able to trust that automation, through software-inherent ethics-rationale reflecting ethical human logic (preferably specified in natural languages) will always behave under strict ethical constraints. These constraints must follow previously defined ethical codes, and be able to limit their actions and behavior under these constraints, always reflecting ethical humans’ instructions, even without human supervision.

The dual challenge in front of us is that as we develop more powerful, intelligent, and autonomous automation, we must also be careful it is not and cannot be abused by unethical people against us and against other people; we must also be careful that this powerful automation does not assume independence to, on its own, hurt people and inflict damage. The challenge for automation scientists, designers, and managers is that we need to consider how to ethically control the behavior of automation and how to ethically restrict its autonomy – because automation is all around us and we are so dependent on it.

### 47.8 Additional Online Resources

Source materials relevant to ethics and automation are available from the ACM and IEEE model curricula, national societies such as ACM, IEEE, AAAS, ASEE, AAES, AIS, and others, for guidelines on ethics; groups such as ACM SIGCAS, CERIAS, CPSR, EFF, EPIC, and other professional organizations that promote responsible behavior. Their conferences, journals and materials provide rich, additional topics on automation and ethics. In addition, the following are several online resources relevant for ethics and automation:

- [http://www.bsa.org](http://www.bsa.org)
- [http://catless.ncl.ac.uk/risks](http://catless.ncl.ac.uk/risks)
- [http://www.cerias.purdue.edu/](http://www.cerias.purdue.edu/)
- [http://computingcases.org/index.html](http://computingcases.org/index.html)
- [http://www.cpsr.org/ethics/eei](http://www.cpsr.org/ethics/eei)
- [http://cseethics.uis.edu/dolce](http://cseethics.uis.edu/dolce)
- [http://www.cyberlawclinic.org/casestudy.htm](http://www.cyberlawclinic.org/casestudy.htm)

- [http://www.dhs.gov/dhspublic](http://www.dhs.gov/dhspublic)
  (on strategy to secure the cyberspace)
- [http://ethics.iit.edu/resources/onlineresources.html](http://ethics.iit.edu/resources/onlineresources.html)
- [http://ethics.iit.edu/codes/engineer.html](http://ethics.iit.edu/codes/engineer.html)
- [http://ethics.iit.edu/emerging/index.html](http://ethics.iit.edu/emerging/index.html)
- [http://ethics.sandiego.edu/resources/cases/HomeOverview.asp](http://ethics.sandiego.edu/resources/cases/HomeOverview.asp)
- [http://www.georgetown.edu/research/hrcbl/nrc](http://www.georgetown.edu/research/hrcbl/nrc)
- [http://microsoft.com/piracy](http://microsoft.com/piracy)
- [http://onlineethics.org](http://onlineethics.org)
- [http://privacyrights.org](http://privacyrights.org)
- [http://www.rbs2.com/ethics.htm](http://www.rbs2.com/ethics.htm)
- [http://repo-nt.tcc.virginia.edu/ethics/index.htm](http://repo-nt.tcc.virginia.edu/ethics/index.htm)
- [http://sceeri.etsu.edu/Ethics.htm](http://sceeri.etsu.edu/Ethics.htm)
  (Modern Wars: Cyber assisted warfare).
47.A Appendix: Code of Ethics Example

ACM (Association for Computing Machinery) Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 47.A.1 outlines fundamental ethical considerations, while Sect. 47.A.2 addresses additional, more specific considerations of professional conduct. Statements in Sect. 47.A.3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Sect. 47.A.4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Sect. 47.A.1, the Code is concerned with how these fundamental imperatives apply to one’s conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computing ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

47.A.1 General Moral Imperatives

As an ACM member I will…

Contribute to Society and Human Well-Being

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

Avoid Harm to Others

Harm means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of computer viruses.

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers,
or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one’s superiors do not act to curtail or mitigate such dangers, it may be necessary to blow the whistle to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

Be Honest and Trustworthy
Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the weight of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

Be Fair and Take Action not to Discriminate
The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

Honor Property Rights Including Copyrights and Patent
Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

Give Proper Credit for Intellectual Property
Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other’s ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

Respect the Privacy of Others
Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.
47.A Appendix: Code of Ethics Example

Honor Confidentiality
The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one’s duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

47.A.2 More Specific Professional Responsibilities

As an ACM computing professional I will...

Strive to Achieve the Highest Quality, Effectiveness and Dignity in Both the Process and Products of Professional Work
Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

Acquire and Maintain Professional Competence
Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

Know and Respect Existing Laws Pertaining to Professional Work
ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one’s actions and for the consequences.

Accept and Provide Appropriate Professional Review
Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

Give Comprehensive and Thorough Evaluations of Computer Systems and Their Impacts, Including Analysis of Possible Risks
Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

Honor Contracts, Agreements, and Assigned Responsibilities
Honoring one’s commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one’s concerns and reasons for that judgment, but failing to procure a change in that assignment, one may
yet be obligated, by contract or by law, to proceed as directed. The computing professional’s ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments against one’s own judgment does not relieve the professional of responsibility for any negative consequences.

**Improve Public Understanding of Computing and Its Consequences**
Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

**Access Computing and Communication Resources only when Authorized to Do so**
Theft or destruction of tangible and electronic property is prohibited by imperative 1.2–Avoid harm to others. Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another’s computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

**47.A.3 Organizational Leadership Imperatives**
As an ACM member and an organizational leader, I will...  

Background Note: This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context leader is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context organizations are corporations, government agencies, and other employers, as well as volunteer professional organizations.

**Articulate Social Responsibilities of Members of an Organizational Unit and Encourage Full Acceptance of Those Responsibilities**
Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

**Manage Personnel and Resources to Design and Build Information Systems that Enhance the Quality of Working Life**
Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

**Acknowledge and Support Proper and Authorized Uses of an Organization’s Computing and Communication Resources**
Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

**Ensure that Users and Those Who Will Be Affected by a System Have Their Needs Clearly Articulated During the Assessment and Design of Requirements; Later the System Must Be Validated to Meet Requirements**
Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.
Articulate and Support Policies that Protect the Dignity of Users and Others Affected by a Computing System

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

Create Opportunities for Members of the Organization to Learn the Principles and Limitations of Computer Systems

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

47.A.4 Compliance with the Code

As an ACM member I will...

Uphold and Promote the Principles of this Code

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

Treat Violations of this Code as Inconsistent with Membership in the ACM

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, Chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtké, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund. This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice. Copyright 1997, Association for Computing Machinery, Inc.

References

47.1 G. Reynolds: Ethics in Information Technology, 2nd edn. (Cengage Learning, Florence 2006)
47.2 H.T. Tavani: Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology (Wiley, New York 2006)
47.5 D.G. Johnson: Computer Ethics, 3rd edn. (Prentice Hall, Englewood Cliffs 2000)
47.8 R. Spinello: Cyber Ethics: Morality and Law in Cyberspace, 3rd edn. (Jones Bartlett, Boston 2006)
47.9 P.M. Asaro: Robots and responsibility from a legal perspective, Proc. IEEE ICRA (2007)
47.10 J.M. Kizza: Ethical and Social Issues in the Information Age, 3rd edn. (McFarland, Jefferson 2007)
47.12 D. Dennett: When HAL kills, who’s to blame?. In: HAL’s Legacy: 2001’s Computer as Dream and Reality, ed. by D. Stork (MIT Press, Cambridge 1996)
47.14 R. Spinello: Readings in CyberEthics, 2nd edn. (Jones Bartlett, Boston 2004)
47.18 K. Himma: Artificial agency, consciousness, and the criteria for moral agency: what properties must an artificial agent have to be a moral agent?, 7th Int. Comput. Ethics Conf. (San Diego 2007)
47.23 G. Stamatekos: Computer Ethics: A Global Perspective (Jones Bartlett, Sudbury 2007)
47.31 M. Dark: Learning and Teaching with Case Studies, Center for Education and Research in Information Assurance and Security (Purdue University, Purdue 2008) http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/course_curriculum/development/ethical_social_prof_issues/learning_and_teaching.php
47.33 I. Asimov: I, Robot (Gnome Press, New York 1950)
47.34 S.Y. Noi (Ed.): Handbook of Industrial Robotics (Wiley, New York 1985)
47.50 Privacy Rights Clearinghouse: San Diego, CA 29103, USA, http://privacyrights.org (last accessed January 2009)
47.51 ComputingCases.org: http://computingcases.org/index.html (last accessed January 2009)

47.55 L.D. Catledge, J.E. Pitkow: Characterizing browsing strategies in the world wide web, Comput. Netw. ISDN Syst. 27 (Elsevier Science, Amsterdam 1995)

47.56 H. Joshi, S. Ito, S. Kanala, S. Hebbar, C. Bayrak: Concept set extraction with user session context, Proc. 45th ACM South East Conf. (Winston-Salem 2007)


47.60 J. Bar-Ilan: Access to query logs – An academic researcher’s point of view, Position paper at Query Log Anal. Workshop at WWW 2007 Conf. (Banff 2007)

47.61 X. Li, E. Agichtein: Towards privacy-preserving query log publishing, Position paper at Query Log Anal. Workshop at WWW 2007 Conf. (Banff 2007)


47.63 L. Weinstein: Search engine privacy dilemmas – and paths towards solution, on line blog entry at http://lauren.vortex.com/archive/000188.html (February 12, 2007)