Feature

Wanbil W. Lee, DBA, is principal director of Wanbil & Associates; president of The Computer Ethics Society; adviser at the Centre for e-Commerce and Internet Law, Vienna; member of the International Expert Network, Nous Global, UK; and adjunct professor at several universities. He has devoted more than five decades to the field of computing, spanning the banking, government and academic sectors, mainly in Australia and Hong Kong. His teaching and research interests focus on ethical computing and information security. Lee also speaks to a wide range of audiences in Asia, Europe and Australia. He is a member of several learned societies and sits on committees/boards of some of those bodies, advisory committees of the Hong Kong government and editorial boards.

Risk and Ethics in Cyberspace

Of all the human inventions since the dawn of civilization, the computer is the only one that extends our intellectual power. All others extend our physical power. The upside is that the computer can bring joy; the downside, misery. There is no problem with joy, but that is not the case with misery. How to minimize the vulnerability, eliminate the threat or mitigate the risk associated with the problem is the question.

IT professionals have been relying on all sorts of countermeasures, including the familiar technical access control mechanisms (such as firewalls, cryptographic algorithms and antivirus software [AVS]), computer law and computer audit, yet organizations still suffer negative consequences. Why is this so? There is something wrong somewhere, but what is it and where does the fault occur? Perhaps our understanding of risk needs be updated; education across science and technology needs be improved; effective decision models need be implemented as the ones currently in use are less than effective; and the Internet community needs to give ethical consideration to developing and using information and communications technology (ICT) products and services.

SHIFTING THE UNDERSTANDING OF RISK TO MINIMIZE MISINTERPRETATION

Security problems—whether of a technical or nontechnical nature—are rooted in human error, to which no one is immune. Wherever and whenever there is vulnerability, there is threat ready to exploit it. Risk will result when threat is actually carried out.

To mitigate risk (that is, the damage, loss or destruction of what one wants to protect), one must deal with vulnerability and identify threat. It can be said that risk is a function of vulnerability and threat \( r = f (v, t) \), and exposure to risk is a function of probability (the likelihood that risk occurs) and damage (of technical, financial and ethical nature) \( r = f (p, d) \).

It has been argued recently that people have long been influenced by the misinterpretation of risk, that risk is taken as a technical concern and measured in economic and legal terms, but it is, in fact, a managerial concern as well and should be evaluated in socio-technical as well as legal-financial terms. This is a mistake and the technical, economic and social aspects should be recognized in order to gain a holistic view.

To make the point, here are several cases for illustration.

Case 1
When planning to replace a corporate legacy system with a web-based facility, concentrating on potential economic efficiency such as improved speed, elimination of redundancy or even reduced head counts means missing such adverse consequences as end-user dissatisfaction and deterioration in morale (due to the disturbance to inertia).

Case 2
Evaluating information governance of a computer-based system, but failing to include an audit of or a check for ethical issues, runs the risk of a deficient information security management review.

Case 3
Assessing softlifting by focusing on the economic and legal impact, such as infringement of copyright law, and leaving out the social impact, such as personal use of sensitive proprietary information, will result in a risk of an incomplete assessment.

Hence, it is important to recast our mind-set and shift our understanding of risk in order to manage risk exposure.

IMPROVING EDUCATION ACROSS SCIENCE AND TECHNOLOGY

Cybercrimes are proliferating and reaching every corner of the world with no sign of slowing down despite the extant preventive measures that comprise technical access control mechanisms and computer laws. Cybercriminals are well educated and equipped with specialized...
knowledge and skills, but they apparently lack a spirit of care for moral justifications. This could be attributed to a flaw in science and technology education that has rendered the teaching/training of science and technology an act of indoctrination with lopsided learning objectives and syllabi dominated by hard, specialized knowledge and skills only. The resultant graduate scientists and technologists become obsessed with short-term technical excellence and economic gain.

The flaw is that the adopted curricula tilt toward technical and economic efficiency vs. long-term, human-centered social acceptability and cultivate a sense of egoistic financial gains, but neglect moral implications. Soft knowledge and skills should be an integral part of the curriculum proper, as they are needed to nurture an awareness of altruistic consequences.

To investigate the impact of education on human behavior in general, and knowledge of computer ethics and students’ attitudes in particular, a seven-year (2006 to 2012) exploratory study, consisting of an annual survey, was undertaken. The empirical data showed that less than 10 percent of the students surveyed claimed that they were aware of computer ethics, more than 60 percent were not sure if they carried out their work ethically, and approximately 30 percent thought that they carried out their work ethically. By deducing from these data, it was concluded that ethics education has a positive impact on the students; that is, knowledge of ethics arguably has an effect of lowering the rate of abuse, and computer science curriculum can be improved by including a module on computer ethics and social responsibility.

### IMPLEMENTING EFFECTIVE DECISION-MAKING MODELS IN CYBERSPACE

Under the dual influences of the misinterpretation of risk and flawed education on science and technology, decision makers invariably focus on the technical, economic and legal variables only, with ethical considerations left out. The resultant decision analysis—composed of cost-benefit and risk analyses—is deficient. To address the deficiency, or to assess social acceptability and detect the possible adverse impact of ethical consequences, the Ethical Movement in Cyberspace (Ethical Movement), which is advocated by the Computer Ethics Society (iEthics), alerts us to a new type of risk (ethical risk), a new category of anti-risk mechanism and a new tool for ethical analysis (Ethical Matrix). It also suggests adding ethical analysis to the decision-making tool kit and to use the Ethical Matrix method for ethical analysis.

### COMPUTER ETHICS

Computer ethics is generally considered a static and passive domain concerned with the social and ethical impact of the computer. Generally speaking, it addresses ethics in cyberspace and is concerned with the ethical dilemmas encountered in the use and development of computer-based application systems. Of course, it is formally defined, and among its many descriptions is Moor’s often-quoted classic definition. The Ethical Movement proposes that computer ethics is not only static, but also dynamic and positive, and represented by a double duality model, depicted in figure 1.

![Figure 1—Conceptual Graph of Double Duality](source: Wanbil Lee. Reprinted with permission.)
COMPUTER ETHICS AS A DIFFERENT TYPE OF RISK
As alluded to earlier, using the computer in contradiction to ethical principles constitutes a different type of risk vis-à-vis risk of a technical, legal or financial nature because risk is a technical and managerial concern and it should be measured in financial, legal and moral terms with equal priority.

COMPUTER ETHICS AS A KIND OF ANTIRISK MECHANISM
Checking for potential ethical impact (in addition to technical and economic efficiency) adds a step, or steps, to the other established antirisk routine countermeasures (including cost-benefit analysis and risk analysis). For example, going through the process of applying the Ethical Matrix method for ethical analysis will force decision makers to consider adverse consequences and may reveal such risk areas as low user morale and dissatisfaction or potentially undesirable consequences of a social or moral nature that would otherwise be missed in the typical antirisk checks and audits. It will also raise technical and economic efficiency issues such as improved speed, elimination of redundancy or reduced head counts. This makes computer ethics a different kind of antirisk mechanism vis-à-vis the extant risk countermeasures.9

These extant countermeasures are being rendered impotent by emerging complex and sophisticated applications and technologies such as the Internet of Things (IoT), big data and cloud computing, and by the ever-lurking perpetrators who are always ready to crack any new countermeasures soon after they are developed and released.10 Antirisk development is becoming more difficult. New antirisk mechanisms are, thus, called for to strengthen the weakened existing mechanisms.

The Internet community is a powerful group in contemporary society as it handles and has under its control a powerful commodity: information. That commodity has an immense impact on our technical, economic, legal and mental well-being. This group has the responsibility to resolve these issues and should realize that ethics is the same in cyberspace as in the physical world, its implication is different. To fill this gap, the Ethical Movement has come up with a new meaning for computer ethics as a risk and an antirisk mechanism. Moving from concept to practice, it has been proposed that this antirisk mechanism be adopted as an alternative anticrime mechanism and as a new approach to evaluating trust.11

THE ETHICAL MATRIX
The Ethical Matrix is a conceptual tool originally designed for making decisions about ethical acceptability of technologies in the field of food and agriculture,12 and the project “Bioethical Analysis in Technology Assessment: Application of the Use of Bovine Somatotrophin and Automated Milking Systems”13 is an early application of the ethical matrix. The aim is to analyze the ethical impacts of injecting subcutaneous bovine somatotrophin (bST), a commercially produced hormone, into dairy cattle in order to increase the milk yields to respond to two concerns: 1) Diminishing well-being of the cattle because higher metabolic demands may lead to increased rates of illness, and 2) Threat to the consumers’ health because of an increase in the milk concentration of insulin-like growth factor 1 (IGF-1).

In general, the matrix is made up of as many rows and columns as the particular case needs. A row is allocated to a stakeholder (an interest group of people, including clients, employers and probably the general public), a column is assigned a “value” representing respect to ethical principles and the cells contain the concerns of the stakeholders (the main criterion that should be met with respect to a particular principle). The method can be applied in two or three steps as follows:

1. Identify and determine the stakeholders, the values representing the respective ethical principles, and concerns of each stakeholder with respect to the ethical principles.
2. Assess/quantify the perceived relative impacts by the identified concerns of the particular interest group with respect to the ethical principles.
3. Debate, deliberate, discuss and decide.

Specifically in the test case, four stakeholders were identified (thus, four rows) humans (food consumers and producers) and nonhumans (farm animals and biota)—and three values were found relevant (thus, three columns):

• Well-being (representing utilitarian values, i.e., “maximizing the good for the maximum number of people”)

Learn more about, discuss and collaborate on computer crime, cybersecurity, risk assessment and information security management in the Knowledge Center.

www.isaca.org/knowledgecenter
• Autonomy (representing deontological values or “treating everyone as ends, not means”—in essence, the Golden Rule)
• Fairness/justice (representing justice in the categorical imperative sense or corresponding to Rawls’ notion of “justice as fairness” [one person’s benefit or gain is consistent with that of others, and fair equality of opportunity, but tolerable of social and economic inequalities for those that would benefit the least advantaged members of society]).

A generic example of an ethical matrix and an illustration of the ethical matrix used in the project can be found in the Ethical Matrix Manual.

It is noteworthy that sometimes the matrix is used for identifying ethical issues only (i.e., step 1 alone). The deliberations and discussions taken to arrive at those issues may contribute helpful hints to the final decision. Further, with appropriate adjustment, the matrix can be adopted for other fields and has been used in other situations. For example, the method was applied to perform an ethical analysis of postimplementation concerns arising from a project for an organization that was replacing its existing offline help-desk platform with an online monitoring system at a high-tech facilities distributor. The concerns thereof are of an ethical nature and include the staff’s concern over personal privacy invasion at work; the firm’s problem with potential damage to corporate image, personnel welfare and staff morale; and the professionalism and deontological issues for the chief information officer (CIO) and the technical team.14

The result of the first-cut analysis is shown in figure 2. Subsequent steps, including quantifying the concerns, evaluating the relative strength or weakness of each concern, and making the recommendation, are not included here in the interest of space. Analysts should note that the underpinning principles mentioned earlier should be consulted in carrying out these steps.

Finally, it is worth noting that the columns and rows may be swapped with each other, giving an alternative structure.15

ETHICAL CONSIDERATIONS FOR THE INTERNET COMMUNITY

ICT professionals of various ranks, including CIOs, tend to offer support when asked for an opinion on the importance of computer ethics, but when pressed for elaboration as to what computer ethics is or why it is important, many may respond in silence. To proceed, a real appreciation of basic ethical principles is needed.

To start, one can look to the Edward Snowden episode. He “blew the whistle.” Some respect him, calling him a hero; others disapprove of his actions, calling him a traitor. Is he defensible on ethical grounds?

One might have heard these arguments: “Snowden is not the only one. There are plenty of other whistle-blowers,” or “If Tom, Dick and Harry can do it, why not Edward Snowden?” These arguments are based on the concept of relativism.16 Hence, if one person thinks it is right to say Snowden is a hero, but another individual does not think so, the argument is pointless, as it allows two people to decide right and wrong for themselves. In the end, no moral distinction between the opinions of the two individuals can be made. Certainly, the debate does not tell us whether Snowden’s actions are morally right or wrong.

But Snowden is no ordinary worker; he is a professional, one who engages in a job that handles a highly sophisticated commodity—confidential information. He was an employee of the US National Security Agency (NSA). In this capacity, Snowden appears to be wrong and disloyal to his employer in stealing and disclosing confidential information without authority. However, while, as a professional, Snowden is expected to respect professionalism and observe his professional code of conduct, as a person, he has a duty to

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Values</th>
<th>Well-being</th>
<th>Autonomy</th>
<th>Justice/Fairness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firm</td>
<td>Personnel welfare, corporate image</td>
<td>Personnel protection</td>
<td>Staff morale</td>
<td></td>
</tr>
<tr>
<td>Staff</td>
<td>Personal privacy</td>
<td>Freedom of personal movement</td>
<td>Exploitation by minority</td>
<td></td>
</tr>
<tr>
<td>Executive vice president</td>
<td>Job security</td>
<td>Firm’s welfare</td>
<td>Entitlement of support resources</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>Corporate policy regarding system utility</td>
<td>Professionalism</td>
<td>Distribution of computer resources</td>
<td></td>
</tr>
</tbody>
</table>

himself and his moral convictions. This duty-based argument is based on the theory of deontology.\(^{17}\)

So, as an employee, Snowden failed because he was disloyal and leaked confidential information. But, as a professional, he was right in exposing the stealth act because he was acting in accordance with professional conduct. While helpful in defending duty-bound actions, this principle is inherently troublesome because the actor owes responsibility to the multitude of stakeholders, and each of the stakeholders has its own aims that may be conflicting with one another.

Next, think of the impact or the consequences of Snowden’s actions. The consequences may be beneficial or harmful. Snowden might have done “good” for the victims in particular and the world at large and “bad” for NSA and the US government. This results-based argument, known as consequentialism or utilitarianism,\(^ {18}\) certainly supplements the duty-based argument, but it leads to questions such as, “How good? How bad? And for whom?”

The consequentialist argument is not sufficient and raises questions about for whom or for how many the result is good. This argument needs to be supplemented with a utilitarian view. A utilitarian argument may be useful to suggest the issue of for whom or what purpose the good result is beneficial or the bad result harmful, but it raises further questions that include, among others, quantifying and comparing the results.

As can be seen, even after taking into consideration the so-called Golden and Silver rules, categorical imperative and social contract theories,\(^ {21}\) none of these principles alone can help resolve ethical dilemmas. Balancing the respect for each principle with the needs of the different stakeholders is necessary to reduce conflicts and arrive at a technically efficient, economically sound, legally viable and socially acceptable solution. A mix of some or all of these principles is needed. The Ethical Matrix could be the answer.

It is important for the Internet community to be equipped with knowledge of computer ethics, especially its role as a different type of risk and an alternative type of antirisk mechanism, and to give ethical consideration to the design and implementation of ICT products and services. Only then can one hope to be truthful to oneself and trusted by all other stakeholders.

**CONCLUSION**

Computer ethics is unlikely to become less important over time. Instead, it is poised to become an increasingly important aspect for those who create applications and solutions and those who use them. While the ramifications of every ethical decision are broad and diverse, a few basic good practices can be defined:

- Know your risk and what it should be.
- Be educated in science and technology. Ensure that your education includes ethics, an oversight in current curricula that needs to improve.
- Know your decision model, including the shortcomings of those in current use and the updated versions.
- Know your ethics. Understand the common ethical theories that underpin computer ethics so you can make up your mind when faced with a case like that of Edward Snowden.
- Know computer ethics, its new meaning and new functions so that you can convince yourself and others to give ethical consideration to the design, development and use of ICT products and services.

**ENDNOTES**

3 “Softlifting” is the software equivalent of shoplifting, which is basically not intended for financial gain and is often mistakenly believed by many to be legal. It occurs, for example, when a person copies a friend’s software or brings a copy of software home from work for personal use. Though commonly considered a category of computer crime, softlifting falls more properly within the area of intellectual property law. Under the US Copyright Act of 1976, it is illegal to make or distribute copies of copyrighted material without authorization. Also, the Act provides a variety of remedies to compensate the plaintiff and punish the offender.
4 *Op cit.*, Lee, 2015
6 The Computer Ethics Society (iEthics), www.iEthicsSoc.org
7 Moor, James H.; *Metaphilosophy*, Blackwell Publishing Ltd, 1985, p. 266-275. “Computer ethics is the analysis of the nature and social impact of information and communication technology, and the corresponding formulation and justification of policies for the ethical use of such technology.”

8 Lee, W. W.; *Ethical, Legal & Social Issues*, Postgraduate Diploma in eHealth Informatics, lecture notes, University of Hong Kong, 2014-15

9 The extant countermeasures can be grouped in the following four categories: technical access control, computer law, risk analysis and computer audit.


13 Ibid.


15 Lee, W. W.; “Pitfalls & Ethical Issues in Internet & Social Media,” Tea Gathering Seminar, organized by the Hong Kong Institution of Engineers for the Veneree Club, 18 September 2013.

16 Ibid.

17 Ibid.

18 Ibid.