GOOD COMPUTING: A VIRTUE APPROACH TO COMPUTER ETHICS

A book under contract with
Jones & Bartlett Publishers
40 Tall Pine Drive
Sudbury, MA 01776
http://www.jbpub.com/

DRAFT FOR
June Puerto Rico writing retreat

Chapter 5
Implementation
Version 1: 04/13/05 by Chuck Huff

Based on writings in www.computingcases.org prepared by Chuck Huff and Bill Frey and class documents from University of Mayaguez, PR, FILO 3185 prepared by Bill Frey

Overview

In previous chapters, we have talked about designing creative ethical solutions, how to test those solutions against ethical standards, and how to think about the complexities of the socio-technical system in which the solutions will be embedded. This last chapter is more focused on the socio-technical system, but specifically on your role as an actor in those systems and how those systems constrain or support your ethical action.

First, we will cover a final test of a solution, the feasibility of that solution in the socio-technical system for which it is proposed. Second, we will look at the role responsibilities a computer professional may take on in an organization. We propose two different roles that in practice often overlap: a) a reactive role of avoiding blame and staying out of trouble and b) a proactive role that views taking responsibility for ethical action as a virtue. We then look at three different kinds of organizations, the roles they pressure computer professionals to adopt, and the match these roles may have with the virtue of taking responsibility.

Finally, we look at what to do if reason fails in your attempts to be a responsible professional in your organization. Ethical dissent ranges from simple attempts at persuasion with superiors to the principled decision to quit your job and blow the whistle on what you believe to be dangerous behavior in your organization. We provide some guidelines for navigating this difficult decision and some advice for how organizations can support ethical dissent internally.

Feasibility Test:

The *feasibility test* focuses on practical constraints in the socio-technical system. It asks whether the proposed solution can be implemented given time, financial, legal, personal, and social constraints. By focusing the decision-maker on these constraints, the feasibility test helps to integrate ethical considerations with other aspects of a decision.

This integration of the ethical and the social is a central point of the socio-technical approach to computer ethics. It is also an important issue for whether or not we can hold a person responsible for an action. The less feasible an action, the less one has an obligation to perform it. There are hard cases where this is not true (where, for instance, one may be required to *try* to do something, knowing it may fail) (ref to Neibuhr).

Steps in Applying the Feasibility Test

Consider each of the following practical constraints that might bear on the proposed action:

- *Time:* Is there a deadline within which your solution has to be enacted? Is this deadline fixed or is it negotiable?
- *Financial:* Are there cost constraints on your solution? Are these fixed or are they negotiable?
- *Legal:* Does your proposed alternative violate any laws or regulations? Are the legal constraints in line with the results of your ethical evaluation? If not, what can you do to align them?

- *Personal:* Do the personalities of the people involved offer any constraints? For example, would your supervisor be open to persuasion, negotiation, or compromise? Or is he or she a dogmatic, close-minded, and inflexible person? Or perhaps too open to persuasion and likely to change?
- *Social, Cultural, or Political:* Consider where your solution is being implemented. How would its impact be viewed through the social, cultural, and political milieu in which it is being enacted? Think of these issues using the several levels of analysis in the socio-technical framework (individuals, groups, organizations, etc.)

Finally, don't treat any of these constraints as absolute; one of the most-used excuses for wrongdoing is capitulation to what appears inevitable. For example, you would like to refuse your supervisor's order to copy illegally the software, but he's really a moral chameleon. Or, you would really like to update the pollution controls on the oil refinery but it's not financially feasible. Constraints appear to set up barriers but moral creativity can often overcome these. Is there really no way to persuade your supervisor to back down? Are there really no cost-effective ways of reducing the refinery's pollution? This capitulation to so-called necessity is really an excuse for poor moral creativity.

Moral Creativity and Gilbane Gold
Gilbane Gold, a video made by the National Society for Professional Engineers, presents a scenario in which an engineer is confronted by an apparent dilemma of blowing the whistle on his company for water pollution or going along with this pollution and participating in a cover-up. For years, those of us who taught this video took this apparent dilemma for granted. Recently however, Michael Pritchard and Mark Holtzapple have published a paper (ref) that presents a technical solution to the problem. In fact they offer several technical options that are more cost-effective than the solution proposed by Z-Corp (the fictional polluter). This paper argues effectively that the main problem is not a dilemma produced by the lack of technical options but the inability to design feasible *and ethical* solutions due to a lack of moral creativity.

Problems, pitfalls, and temptations with the Feasibility Test
Allowing illegality to determine immorality. Many of us think that legal requirements trump ethical ones. In this version of the trump, we think that if the law forbids something, then it is immoral. For example, during a workshop, we discussed the propriety of sending emails to family and friends during work time. A participant offered the following as a conversation stopper: "It is wrong to do this because it violates Puerto Rican law; in Puerto Rico it is expressly forbidden for government employees to use workplace facilities to send emails to friends and family." In response, several participants distinguished the legal and the ethical. Moreover, a student once pointed out to us that while working for a U.S. government agency during a summer internship, he was allowed to use their facilities to send emails to family, since it represented an effective way for him to stay in touch. Was it wrong for him to so this, even though he had his employer's permission? Was the U.S. government agency wrong to allow him to do so, since this action violates Puerto Rican law?

Remedy: Often we fall into this trap because we don't use our moral imaginations. We uncover the legal rule and simply say, "Well, there's your answer!" And since we have an answer, we do not need to do the difficult work of thinking carefully about our moral obligations. In doing this, we forget that the law and ethics are distinct—although overlapping—we cannot infer the ethical from legal; nor can we infer legal from ethical.

The appeal to the legal to settle an ethical dispute is often employed in bad faith as a strategy to win a debate by deciding it before it gets started. (This is why we call these appeals, "conversation stoppers.") There are two things you can try in this case. First, bring in the other tests (reversibility, harm, publicity, code), and emphasize that what they have to say should be considered on its own merits independently of the legal test. In fact, the ethics tests can be used as an independent check on the legal pronouncement; sometimes laws are simply wrong, unjust, unethical. Second, to get the conversation going again point out instances where the legal and the ethical diverge. For centuries in Europe, collecting interest on loans was illegal. It still is in many religious codes (e.g. Islam). It is now inconceivable that it would be made illegal in the West (or in most other places, for that matter).

Allowing legality to determine morality. "But it is perfectly legal to insert code into this program that allows me to disable it when the client does not pay!" This is a variation of the earlier temptation. The temptation is to think that since the law permits something, then one is allowed to do it or even justified in doing it. This temptation often produces great effort and creativity in seeking a legal way to do what one know is likely unethical. But finding a legal way to do it allows one the fig leaf of respectability in what is really the action of a moral opportunist.

Remedy. Consider Tulkinghorn's example. In Charles Dickens' novel, *Bleak House*, the lawyer Tulkinghorn brought about his Machiavellian ends while acting under the shield of legality; the fact that something is legal does not make it moral. Dickens has little love for lawyers (a feeling we do not share) and he made Tulkinghorn's villainy obvious. Slavery and apartheid were both legal at one time; they are (and were) also wrong. In fact the public debates that led to their overthrow were largely fueled by *independent* ethical argument.

Allowing financial constraints to determine morality. By now you will have noticed a pattern in these headers. This mistake involves missing the fact that choices in budgets are based on the mission, values, and resources of the organization. So, choices in budget, like many choices in software design, are moral choices. Still you may have little control over those choices and how they are made.

Remedy. The remedy again is more moral creativity. Try to imagine ways that issues can be resolved within the budget constraints. Don't let budget constraints short-circuit your moral creativity. If you go back to the ethics tests, or to your socio-technical analysis you may find other constraints that actually trump budget constraints (e.g. legal requirements for disability accommodation may persuade management to allocate budget lines for this).

Allowing obligations to the employer to determine morality. In many ways, this is a variant of the computer professional as "hired gun" approach that we discussed in chapter one. Some moral opportunists (see vices of defect in reasonableness on page X) may argue that their responsibility to their client (or their employers or manager, or to the shareholders) trump all other ethical obligations. They are acting merely as the agent of the other. On page X we have shown how this argument can become a moral distancing device to avoid responsibility for even such heinous things as genocide. And if your role as the agent for someone else is the *only* obligation you will claim, you will have to be willing to justify complicity in genocide. Once you admit exceptions, we are back in the game of balancing moral goods against each other.

Remedy. Again, balancing the influences on the decision among the moral, legal, etc. constraints is the answer. This involves bringing back in the ethics tests, and using moral creativity to construct solutions that satisfy your obligations to the employer and to other parties in the socio-technical system.

Feasibility and ethical responsibility

This general form of the traps we cover here is that of taking on the false mask of "realism" and only considering one of the dimensions of feasibility, and not considering any of the moral aspects. Thus, this trap applies to the relation of ethics to all the other feasibility fields. For example, business practitioners often assume without question that financial matters trump ethical matters. Those who disagree are labeled unrealistic. Environmental concerns are assumed incompatible with business objectives; the environmental advocate is asked how he could possibly hold that environmental concerns are more important than jobs (Why are environmental concerns opposed to business goals? Can we do both?). Here are some strategic responses to these kinds of arguments:

1. *The ethical is distinct from the legal, technical, financial, etc*. Thus the ethical cannot be reduced to these other realms. So demand that your interlocutor put forth an ethical as well as a legal, economical, or technical justification.
2. The ethical is distinct from these other realms but it also overlaps with them. Thus, the ethical informs the legal, guides the technical, and limits the pursuit of the financial. *This overlap shows us that the ethical is not automatically opposed to the legal, the technical, the financial, etc*. So the ethical cannot be set aside because financial considerations dictate it. (When they are in conflict, the ethical should win out; but who says we can't often have both?)
3. *The burden of proof should fall on those who try to set aside the ethical because it is not feasible*. Why can't we find a financially feasible, *ethical* solution to the problem? Why should the ethical be reduced to the legal or give way to the financial? Why are ethical considerations incompatible with manufacturability or technical considerations? Aim first for synthesizing, combining, balancing, or harmonizing the ethical with other considerations. Only after a thorough search discuss trade offs and compromises. And always formulate trade offs with a non-negotiable ethical bottom line. Burden of proof problems are often significant ones in organizations, since anyone who wants to change policy often is required

to take on this burden, while those who resist change are not required defend the ethical import of this.

The Responsible Computing Professional

Let's start with a scenario, a decision-making moment from the Hughes Aircraft Case:

> *Frank Saia has worked at Hughes Aircraft for a long time. Now he is faced with the most difficult decision of his career. He has been having problems in the environmental testing phase of his microchip manufacturing plant; the detailed nature of these tests has caused Hughes to be consistently late in delivering the chips to customers.*
>
> *Because of the time pressure to deliver chips, Saia has been working to make the production of chips more efficient without losing the quality of the product. Chips are manufactured and then tested, and this provides two places where the process can bottle up. Even though you might have a perfectly fine chip on the floor of the plant, it cannot be shipped without testing. And, since there are several thousand other chips waiting to be tested, it can sit in line for a long time. Saia has devised a method that allows testers to put the important chips, the "hot parts," ahead of the others without disrupting the flow and without losing the chips in the shuffle. He has also added a "gross leak" test that quickly tells if a chip in a sealed container is actually sealed or not. Adding this test early in the testing sequence allows environmental testing to avoid wasting time by quickly eliminating chips that would fail a more fine-grained test later in the sequence.*
>
> *Because environmental testing is still falling behind, Saia's supervisors and Hughes customers are getting angry and have begun to apply pressure. Karl Reismueller, the director of the Division of Microelectronics at Hughes, has given Saia's telephone number to several customers, whose own production lines were shut down awaiting the parts that Saia has had trouble delivering. His customers are now calling him directly to say that "we're dying out here" for need of parts.*
>
> *Frank Saia has discovered that an employee under his supervision, Donald LaRue, has been skipping the tests on the computer chips. Since LaRue began this practice, they have certainly been more on time in their shipments. Besides, both LaRue and Saia know that many of the "hot" parts are actually for systems in the testing phase, rather than for ones that will be put into active use. So testing the chips for long-term durability that go into these systems seems unnecessary. Still, LaRue was caught by Quality Control skipping a test, and now Saia needs to make a decision. Upper management has provided no guidance; they simply told him to "handle it" and to keep the parts on time.*

He can't let LaRue continue skipping tests, or at least he shouldn't let this skipping go unsupervised. LaRue is a good employee, but he doesn't have the science background to know which tests would do the least damage if they were skipped. He could work with LaRue and help him figure out the best tests to skip so the least harm is done. But getting directly involved in skipping the tests would mean violating company policy and federal law.

This scenario helps set forth two frameworks for responsible computing, one articulating a minimal level of responsibility (blame-avoidance) and another articulating an exemplary standard of responsible computing (responsibility as a virtue). The best way to understand these frameworks is to see them in action, so both frameworks will be used to chart courses of action for Frank Saia.

Framework 1: Staying out of Trouble

The morally responsible computing specialist successfully carries out professional and ethical responsibilities even under difficult circumstances. Responsible computing involves two related frameworks, one reactive and the other proactive. Each framework rests on theoretical foundations summarized in various textboxes. The first establishes a minimal level of responsible computing practice. Consider the following four sets of questions:

- What are Saia's **role responsibilities** in this situation? Is it possible to carry out all of them?
- What factors could **limit his ability to execute** these role responsibilities? Does he lack certain capacities? Does he lack the organizational power or authority to carry them out? Does the situation present constraints that restrict options and make action difficult?
- How can Saia avoid **moral fault** in this situation?
- In general, what can Saia do to emerge from this situation as a **minimally morally responsible agent**? How does he disassociate himself from the wrongdoing and harm that could emerge from this situation?

These four groups of questions arise out of the first responsibility framework. Let's examine each in more detail.

Textbox: Senses of Responsibility

'Responsibility' is used in several distinct ways that fall under two broad categories, the reactive and the proactive. **Reactive** uses of responsibility refer back to the past and respond to what has already occurred. **Proactive** uses are future oriented and attempt to control what happens in the future.

Reactive Senses:

1. ***Causal Responsibility*** refers to prior events (causes) which produce or prevent

subsequent events (effects). The tornado (cause) blew off the roof of the house (effect).

2. ***Role Responsibility*** delineates the obligations individuals incur when they commit to a social or professional role. When individuals become computing professionals they commit to certain obligations, many of which are spelled out in professional codes of ethics. Managers in organizations have a role and responsibilities that go with that role.
3. ***Capacity Responsibility*** sets forth those conditions under which someone can be held (blame) responsible for their actions.
4. ***Blame Responsibility*** determines when we can legitimately praise or blame individuals for their actions.

Proactive Senses:

1. ***Sharing Responsibility*** sets forth those conditions under which we can *legitimately* feel pride and shame in, or responsibility for, actions performed by others to whom we are attached by relations of solidarity. It also refers to the conditions under which we take on additional obligations or (role) responsibilities for tasks that others have left undone.
2. When responsibility is treated ***as a virtue***, it becomes proactive and refers to the supererogatory, i.e., that which goes beyond minimum duty. Those who practice responsibility as a virtue make special efforts to…
    - defuse blame avoidance strategies
    - design role responsibilities with overlapping domains
    - extend the scope and depth of knowledge
    - amplify control and power
    - adopt problem-solving approaches based on design methodology

Exercise*: Identify the different senses of responsibility used in the following paragraph. Some uses employ more than one sense.*

Frank Saia was **responsible** for ensuring that the computer chips were delivered on time and that they were properly tested according to military specifications. When deliveries fell behind schedule, his supervisor, Karl Reismueller, held him **responsible** for the delays and gave his phone number to the angry customers. These customers held Saia **responsible** for having to shut down their production lines until the missing chips were delivered. Saia, on the other hand, claimed that the delivery dates were unrealistic given the technical constraints of manufacturing and testing the chips; this relieved him of **responsibility** for the delays. Should the military find that Hughes had not carried out their responsibilities as stated in the contract, Saia would be targeted and held **responsible** for Hughes losing the contract. As result, he would be dismissed or demoted.

Margaret Gooderal felt **responsible** for ensuring that the computer chips were properly tested and free of defects; she treated them as if they were her own chips, feeling proud when they were of good quality and shame when they fell short of standards. When she

discovered that LaRue was skipping tests, she took upon herself the **responsibility** of informing Saia and other supervisors of the problem. She also felt **responsible** for helping members of the environmental quality control team who were distressed when LaRue insisted that they "pass" chips that had failed the environmental tests. They identified her as a **responsible** person to whom they could turn for help. On the other hand, Margaret Gooderal's supervisors held her **responsible** for raising all kinds of problems; they branded her a trouble-maker.

1. Role Responsibility

The concept of *Role Responsibility* covers the obligations individuals have because of the social and professional roles they occupy. To help identify these, we present the following five sources of role responsibilities:

- Explicit commitments such as **contractual obligations** and **promises**. Individuals commit to formally specified obligations when they sign contracts. Hughes committed to providing chips that conformed to certain specifications. They also committed to testing these chips in certain ways and to delivering them within specified deadlines.
- Implicit commitments embedded in our **social relations and roles**. Being a parent implies all kinds of commitments that cannot (and should not) be specified in advance; attending PTA meetings, taking children to drama practice, spending the morning in the doctor's office to seek care for a sick child, etc. These commitments cannot be predicted in advance but emerge as certain situations develop.
- **Legal Responsibilities**. Computing professionals must honor property rights. This is both a professional and a legal duty. Another legal responsibility that applies to Saia would be the responsibility of ensuring that computer chips manufactured by Hughes pass the specified environmental tests.
- **Job Description**. Computing professionals work as employees occupying organizational positions that are at least partially defined by job descriptions. Saia's job description included monitoring the activities of employees under his supervision. It also included overseeing delivering computer chips within the deadlines specified. (Did it include responding to customers angry at delays in delivery of product or did this responsibility fall on Saia's supervisor, Karl Reismueller?)
- **Codes of Ethics**. Computing professionals have many responsibilities spelled out in their codes of ethics. An example would be the responsibility to "contribute to society and human well-being" that is spelled out in imperative 1.1 in the ACM code of ethics. After stating this general provision, the code highlights some of its aspects, for example the responsibility to "minimize negative consequences of computing systems". These specifications, which are presented in general form, require interpretation when they are enacted in concrete situations. For example, how should Saia go about minimizing the negative consequences of computing systems? Would this oblige him to ensure that all the chip environmental tests are

carried out? Is minimizing harm consistent with skipping tests on chips that would not be used in safety critical systems? Would it include passing chips that have failed tests if these chips were to be used only, say, in testing prototypes?

These five points provide a checklist of the roles and associated obligations that a computing specialist must carry out. A quick glance shows that conflicts arise between different roles and their attendant obligations. Saia's job responsibilities may come into conflict with his professional responsibilities. A single role may give rise to conflicting obligations. For example, as a Hughes supervisor, Saia is responsible for delivering the chips to the customers on time and for ensuring that all of these chips are tested, two obligations that proved difficult to balance. So ethics codes show how conflicts arise between roles and within roles. While professional codes contain valuable suggestions on how to resolve these conflicts, much of responsible computing involves finding creative solutions to resolving these conflicts.

Textbox: Role Morality

Notice that the role responsibility perspective assumes that the social or professional role itself is morally justified. But this is not necessarily the case. Consider roles like Nazi prison camp guard, torturer of political prisoners, and Mafia hit man. The obligations attached to these roles are immoral because the roles themselves are immoral. So we need to evaluate the morality of social or professional roles as a whole. How do we go about this?

Fortunately, we already have a suitable framework. We evaluate roles and their obligations by using the ethics tests we discussed in chapter eight. For example, after identifying a role's stakeholders, we could ask whether that role is reversible, harm minimizing, and publicly identifiable in reference to these stakeholders. We could also evaluate roles using the theories that underlie the ethics tests. Does a role accord with deontological principles? Is it consistent with basic human rights? How does it stand with the principle of utilitarianism? Is this role consistent with the virtues of the MECP (Morally Exemplary Computing Professional)?

It is important that we subject professional roles to an overall ethical evaluation. Think about the computing profession. Does it stand up to ethical scrutiny?

- Who are the stakeholders of computing practice?
- Are computing practices reversible with these stakeholders?
- Do these practices minimize harm and maximize benefits for society as a whole?
- Are computing practices consistent with civic and moral virtues? (Responsibility, honesty, justice/fairness, and integrity are good places to start.)

2. Identifying factors that limit the ability to execute role responsibilities.
Factors that limit our ability to carry out our role obligations give rise to moral excuses. There are times when we are unable, for legitimate reasons, to carry out our responsibilities. Unforeseeable circumstances force people to act out of character. (A usually prompt person is late because he helped a stranded motorist change a flat tire.) Our actions—through no fault of our own—produce results that are contrary to our expectations and intentions. Actions occasionally miscarry. In these situations, excuses are necessary and justifiable. But the existence of excuses creates opportunities for those who would act with impunity. So we need to identify when excuses are necessary and legitimate, and—at the same time—to limit their range to thwart those who would exploit them to act without answering for their actions.

In general, excuses group themselves around two types. First, there are circumstances which compel us to act against our wills. I signed the contract but I did so against my will. My nemesis pointed a gun at my head. Absent this compelling condition, I would have done otherwise. Second, we cannot act responsibly if we are ignorant. I betrayed my friend's secret. But when he told me the sensitive information, he neglected to tell me that it was a secret. Because I acted out of ignorance, I cannot be blamed for the results.
In the following table, we present excuses relevant to the computing context. The first column cites the condition forming the basis of the excuse. The second presents the corresponding excuse:

Excuse Source	**Excuse Statement**
1. Conflicts within a role responsibility and between different role responsibilities	I cannot, at once, carry out all my conflicting role responsibilities
2. Hostile Organizational Environment (routinely subordinates ethical to financial and other non-ethical considerations)	The environment in which I work makes it impossible to act responsibly. My supervisors overrule my ethical and professional judgment, and I don't have the power to contest this.
3. Overly determining situational constraints: financial and time	I lack the time and money to carry out my responsibility.
4. Overly determining situational constraints: technical and manufacturing	Carrying out my responsibility goes beyond technical or manufacturing limits.
5. Overly determining situational constraints: personal, social, legal, and political	Personal, social, legal, or political obstacles prevent me from carrying out my responsibilities.
6. Knowledge limitations	I lack the knowledge to act effectively and responsibly in this situation.

There is an important limitation surrounding excuses and their sources. For example, Saia may have been ignorant of the fact that LaRue was skipping tests. Yet this ignorance could be attributed to Saia *as a fault*; as LaRue's supervisor, *he should have*

known what his subordinate was doing. In this case Saia's ignorance is not excusable because it was brought about by his own past actions; he was ignorant because he didn't take the appropriate effort required to know the crucial information. A similar line of argument applies to the other circumstances mentioned in the table. For example, there may not have been enough time to test all of the chips and still remain within the delivery deadline. But why, in the first place, was so little time allotted for the testing? Perhaps Hughes officials promised unrealistic deadlines to get the contract. Perhaps they were overly optimistic, intentionally deceptive, negligent or reckless in projecting their deadlines. In general, if the condition that blocks responsible action in the situation (say, ignorance or compulsion) was caused by a prior faulty action (say, negligence or recklessness) then the agent cannot claim a legitimate excuse.

3. Identifying and Avoiding Moral Fault.
The idea that wrongful actions stem from moral fault leads us to the next part of the framework. We can identify three kinds of moral fault that block moral excuse claims:

- *Wrongful Intention*: acting with the express intention of violating a civil or moral law
- *Negligenc*e: unknowingly but faultily creating a risk (usually by not exercising due care)
- *Recklessness*: knowingly creating an unreasonable risk to oneself or to others

Responsible computing requires avoiding moral fault; prior to acting, we must carefully examine our motives and intentions. Are we about to perform an action motivated by a desire for revenge, unbounded ambition, or an unlimited sense of competition? Then it must be set aside because these motives give rise to wrongful intentions. Finding questionable motives is often difficult because they are covered by layers of self deception and rationalization. We must take special care to expose and eliminate them. In addition, we practice due care (and avoid negligence) by taking reasonable precautions to detect and correct error. The meaning of 'reasonable' is difficult to pin down, but it generally means those precautions that a normal, competent computing professional would take in a similar situation. Finally, we must avoid knowingly imposing undue risks on ourselves or others, even in the pursuit of things that in other respects are good. LaRue's goal of getting the chips out on time was praiseworthy; but the risks he imposed by skipping the tests constituted the moral fault of recklessness.

Devising and documenting a minimally acceptable course of action demands paying close attention to the elements of this framework. To avoid blame, we must clarify and limit our role responsibilities and make every reasonable effort to carry them out. Should we not be able to do so, then we need to document morally legitimate reasons such as ignorance and compulsion. Finally, we must demonstrate that we have exercised due care and have worked to avoid moral fault. Staying out of trouble does not prevent trouble. But it provides a minimal basis upon which to build the other components of responsible computing.

Framework 2: Responsibility as a Virtue

Does responsible computing require more than just blame-avoidance? The answer is yes when we expand our concern beyond staying out of trouble to preventing trouble and doing good. But with this broader concern, the notion of responsibility seems to advocate two contradictory paths:

- *To avoid blame, we need to **reduce** the sphere of our responsibilities.* Staying out of trouble requires (1) restricting the range of our role responsibilities and clearly distinguishing ours from others; (2) limiting what we know about a situation to claim ignorance should it turn out badly; and (3) pointing to lack of control and power to claim the excuse of compulsion. In short, we avoid blame by limiting the scope of responsibility.
- *To avoid harm, we need to **expand** the sphere of our responsibilities.* Corporate studies in accident prevention show that the best policies encourage employees to uncover and correct the errors that lead to accidents. This requires moving beyond punishing error to rewarding those who discover and correct error. To go even further, we have discovered that avoiding harm requires (1) expanding the range of our role responsibilities and sharing tasks with others so that we can take up the slack should they fail; (2) expanding what we know about the situation to prevent accidents arising from ignorance; and (3) expanding employee participation in decision-making through empowerment programs. In other words, avoiding error requires that we do just the opposite of what we should do to avoid blame; we must take on more—not less—responsibility.

The proactive sense (preventing trouble) of responsibility seems to contradict the reactive sense (staying out of trouble). But this apparent contradiction disappears when we focus on the different aims of these two responsibility-types. The primary goal of reactive, blame responsibility is to respond to accidents caused by moral fault; deterring future occurrences is only a secondary aim that sometimes follows from punishment. On the other hand, proactive responsibility begins with the absence of fault. It seeks to prevent accidents from ever arising by uncovering embedded problems and designing counter-measures. So it requires pushing back the limits to responsible action by reducing ignorance, expanding control, and sharing role responsibilities. Each sense has its proper domain and breaks down when applied outside that domain. Reactive blame responsibility falls short when we seek to prevent trouble, while proactive responsibility does not address the need for blame assignment and deterrence. It is important to distinguish these senses (by distinguishing their basic aims) and then restrict the use of each to its proper domain.

There are three reasons why the blame responsibility is inadequate for exploring the proactive dimension of responsible computing. First, blame-avoidance strategies fail to prevent what are called "normal accidents." (Ref: Perrow and Reason) Second, assigning blame becomes impractical with complex technologies because of the problem of "many hands." (Ref: Nissenbaum in Johnson) Finally, overemphasis on blame avoidance leads to the self-destructive strategy of *see no evil, hear no evil, and do no evil.*

This strategy is tragically self destructive when dealing with modern complex computing because doing nothing in this context is the best way to bring about trouble.

Blame-avoidance fails to prevent a new type of accident that has emerged with the development of complex modern technology. Charles Perrow, in a study motivated by the near melt-down of the nuclear reactor at Three Mile Island, calls these loss-of-control incidents, "normal accidents." Everyday events, insignificant by themselves, interact in unpredictable ways to produce a rapidly occurring series of interrelated failures that combine to form major catastrophes. Three Mile Island, for example, began with a minor incident, the blocking of a resin filter during a routine maintenance operation. Technicians failed to isolate this incident because of the "tightly coupled" reactor system. This caused a series of spreading mishaps that combined to produce a massive reactor failure, the release of radio active elements, and a near meltdown.

Reactive, blame-centered approaches fail to deal with normal accidents that typically occur in the absence of moral fault. We prevent normal accidents by encouraging systems operators to take an aggressive, proactive, and preventive stance. Avoiding moral fault is not enough here; preventing accidents requires a heightened sense of care, responsibility, and vigilance. Nancy Levesen (ref) makes this argument eloquently in her text *Safeware*, and provides numerous cases of software failure in safety critical systems.

The problem of "many hands" is closely linked to the problem of normal accidents. Normal accidents result from several interrelated actions performed by large numbers of people. Singling out one—or even a limited number of—agents for blame is impractical in these situations. Blame, after all, requires clear, linear causal sequences so that one can infer back from the accident to the actions of a few causally contributing individuals. But, as Perrow points out, the causal sequences in normal accidents are non-linear; assigning an agent to an action becomes next to impossible. Without causal responsibility there is no blame responsibility. Thus, the phenomenon of many hands makes blame assessment impractical.

This brings us to the third difficulty: pushing blame responsibility to its ultimate conclusion leads to an obsession with blame avoidance. We start by recognizing that normal accidents do happen. Then, because they result from freakish sequences of events, we conclude that they are unpredictable and, therefore, beyond our control. Armed with this fatalism, we embrace blame-avoidance; since we cannot prevent normal accidents, we emphasize protecting ourselves from blame. If you can't prevent the accident, then avoid becoming the scapegoat. Adopting a *see no evil, hear no evil* approach (cultivated ignorance) bolstered by a *do no evil* approach (cultivated powerlessness) seem the best strategies for avoiding blame.

Let's look at this more closely. First, under blame responsibility, knowledge aggravates blame while ignorance lessens or eliminates it. So a good blame avoidance strategy is to remain ignorant. Don't seek bad news. If someone tries to bring you bad news, shoot the messenger. Eventually people will stop bringing you bad news. Second, power and authority aggravate blame while compulsion (brought about by a lack of authority and

power) lessens or eliminates it. So another effective blame avoidance strategy is to avoid power and authority. Should something untoward occur, you can show you were powerless to prevent it and point the finger of blame at someone else.

Two blame avoidance strategies were at work in the Hughes case. Saia felt better off not knowing that LaRue was skipping tests. So when Goodearl brought him the bad news, he responded by shooting the messenger; he threatened Goodearl with dismissal rather than responding to her concerns. Reismueller, Saia's supervisor, also employed a blame-avoidance strategy. When customers complained about delayed shipments, he referred them to Saia. It was Saia's—not his—role responsibility to get the chips out on time. He provided Saia with no advice on how to do this; he merely reiterated that Saia had to get the chips out on schedule. The Hughes case reveals a blame-avoidance strategy pushed to the extreme. It also demonstrates that blame avoidance fails to prevent trouble. Clearly, something better is required.

Normal accidents, the phenomenon of "many hands," and wide-spread blame-avoidance strategies all point to the need to broaden the notion of responsibility. With this in mind we turn to how responsible computing professionals should go about preventing harm. Fortunately, moral theory provides us with a concept that we can use to map out this new, proactive region. Preventing harm and doing good require that we explore responsibility as a *virtue*, that is, as a characteristic of human excellence that goes above and beyond blame and punishment.

Mapping out responsibility as a virtue seems a formidable task. But we can begin with the excuses we identified in the blame-centered responsibility framework. Since these represent limits that prevent responsible action, we can characterize responsibility as a virtue as pushing back or eliminating these impediments. We have already identified impediments to responsible action: (1) overemphasis on blame-avoidance, (2) separate and limited role responsibilities, (3) ignorance, (4) compulsion, and (5) situational boundary constraints (such as time limits and technical feasibility) that impose upon us unethical trade offs. So we can chart out the region of responsibility as a virtue by reexamining these limits and identifying strategies for reducing or eliminating them. After this, we will, following Aristotle, present the virtue of responsibility as the *mean* between two extremes, that of *excess* (trying to take on too much responsibility) and *defect* (too little responsibility or irresponsibility).

1. Preventing accidents and uncovering embedded errors require a proactive, aggressive, and activist approach. We begin by *setting aside blame avoidance strategies*. Seeing, hearing, and doing no evil may keep you out of trouble. (But don't bet on it!) Nevertheless, they fail to prevent trouble.
    a. **Ways to defuse blame-avoidance strategies**: *Replace fear of punishment with care and pride. Broaden participation in problem-solving by sharing responsibility with others. Restrict blame and punishment to moral fault. Work proactively to anticipate and prevent system breakdowns and failures.*

2. Establishing a one-to-one relation between untoward actions and blameworthy agents requires clearly defined and sharply delineated role responsibilities. But this does not prevent problems arising through the gaps between role responsibilities. A proactive responsibility framework requires *overlapping role responsibility domains* to encourage individuals to work together in spotting and correcting accidents and errors. Redundancy in the area of responsibility prevents problems and accidents from arising.
    a. **Ways to promote the development of overlapping role responsibilities**: *Set aside blame-avoidance. Cultivate pride, shame, and responsibility for the results of group work. Turn the problem of many hands into an opportunity; if many hands contribute to problems, many hands can also cooperate to prevent or resolve problems. Use a team approach to accident prevention.*

3. Ignorance provides the basis for morally legitimate excuses. But, taken to its extreme, it creates the "see no evil, hear no evil" attitude. Responsibility as a virtue requires adopting *strategies for reducing ignorance by deliberately seeking out "bad news."* Try to find bad news as early as possible. The earlier response is almost always more effective than a delayed one.
    a. **Ways to extend the scope and depth of knowledge**: *Adapt a preventive stance that uncovers risk and draws out error. Encourage bad news instead of shooting the messenger. Work to continually improve professional knowledge and skills. Present options/solutions along with problems when communicating "bad news."*

4. Compulsion provides another basis for morally legitimate excuses since we cannot act responsibly when we fail to overcome circumstances that block, thwart or cause our actions to miscarry. Responsibility as a virtue moves to prevent compulsion by anticipating it and working proactively to extend control and enhance power. We push back circumstances that restrict action and implementation. Instead of pointing to limitations to "get off the hook", we push these back, strengthen our capacities, and take on more, not less, responsibility.
    a. **Ways to extend control and power**: *Work to participate more broadly in decision-making. Advocate ethical and professional standards in decision-making. Work to strengthen technical knowledge and skills. Act collectively to support professionals who are being pressured to violate ethical and professional standards.*

5. Finally, blame-avoidance strategies work best in situations with only limited options for actions. The more options we have, the more responsible we become; the more responsible we become the more vulnerable we are to blame. On the other hand, responsibility as a virtue encourages us to work to expand possibilities for actions by exercising moral imagination and "thinking outside the box". Instead of throwing up our hands at conflicts that arise between role responsibilities, important values, and rigid situation constraints, we need to adopt a proactive stance that leads us to seek ways of *synthesizing conflicting*

responsibilities and values as well as *pushing back and defusing situational constraints*. Many of these optimizing methodologies have been worked out in design approaches to problem-solving. So responsibility as a virtue requires *adopting a design methodology of problem-solving*.

a. **Ways to implement a design-based problem-solving strategy**: *Avoid polarizing issues. Think outside of the box. Exercise moral creativity and practical imagination. Start by trying to synthesize conflicting values. Develop creative ways to push back constraints.*

This provides a sketch for developing a different approach to responsibility that replaces reaction with pro-action. With this in mind, we can now outline how responsibility is structured as a virtue by showing defect, excess and mean in the following textbox:

Textbox: Responsibility as a Virtue

Responsibility as an Aristotelian virtue, i.e., as the mean between the extremes of defect and excess

Defect	**Mean**	**Excess**
Responsible computing is nothing but staying out of trouble	Responsible computing requires defusing blame-avoidance strategies	In responsible computing, we are all to blame for what goes wrong
One-to-one relation between an individual and a role responsibility	Design overlapping role responsibility domains (build in role redundancy)	No distinction between domains; everyone is role responsible for everything
See no evil, hear no evil	Extend scope and depth of knowledge	Postpone any action until you know everything
Do no evil by doing as little as possible	Extend control & power	Delegate nothing to others; try to do everything yourself
All problems are dilemmas that require that we choose between mutually exclusive values	Design-based problem-solving strategy that seeks value synthesis first, compromise second, and trade offs only as a last resort	A refusal to acknowledge that some situations may require compromise or trade offs (There are times when we are confronted with true dilemmas.)

Textbox: Two Responsibility Frameworks

Minimal Responsibility (Staying out of Trouble)

1. *Identify and carry out role responsibilities*
2. *Identify situational factors that limit the ability to execute role responsibilities. (These are factors that compel our actions or contribute to ignorance of crucial facts about the situation.)*
3. *Avoid moral fault by eliminating wrongful intentions or motives, exercising due care, avoiding negligence, and avoiding recklessness.*
4. *Design a course of action that, among the limited alternatives offered by the situation, represents the least harmful as well as least morally objectionable alternatives.*

Responsibility as a Virtue (Preventing Trouble)

1. *Defuse blame avoidance strategies*
2. *Design responsibilities with overlapping domains*
3. *Extend the scope and depth of knowledge*
4. *Extend control and power*
5. *Adapt an aggressive problem-solving approach based on design methodology*

Corporate Environments, and Shifting Role Responsibilities

Two very different studies discuss how corporations treat professional employees. Robert Jackall, a sociologist, studied several large corporations in the early 1980's and published the results in his book, *Moral Mazes: The World of Corporate Managers*. A second study carried out about 10 years later, called the Hitachi Report, looks at the relation between managers and professional engineers in several companies in the Chicago area. Michael Davis reports the results in Chapter 9 of *Thinking Like an Engineer: Studies in the Ethics of a Profession*. From these two sources, we can identify three working environments distinguished by the company's central objectives: (1) **finance-driven** companies that give priority to realizing financial goals such as maximizing profits; (2) **quality-driven** companies that recognize financial issues but believe that these are best realized by producing high quality products and services; and (3) **customer-driven** companies that believe that the road to success lies in identifying and fulfilling customer needs.

There are only minor differences between quality-driven and customer-driven companies. In customer-driven companies, professional and ethical considerations are not as thoroughly integrated into the company's central objectives as in quality-driven companies. Moreover, in customer-driven companies, there is a sharper distinction between professionals and managers. The upshot of these differences is that professionals in customer-driven companies have a greater responsibility to advocate professional and ethical considerations in the decision-making process. As one manager put it, we expect engineers to "go to the mat" in defending safety in the decision process. In quality-driven companies, ethical and professional considerations are thoroughly integrated into the company's central objectives. Hence, the responsibility for advocating ethical and professional considerations becomes unnecessary. It is replaced by the general challenge of integrating ethical and professional considerations with non-ethical considerations such as financial, technical and manufacturing values. Since the difference between advocating and integrating ethical and professional values is fairly minor when it comes to actual practical, we will treat customer-driven and quality-driven companies as more or less the same in the following analysis.

These two studies allow us to compare finance-driven and customer/quality-driven companies. We will exam five key areas: (1) the different roles that managers and

professionals play in decision-making, (2) the contrasting ways in which each organization-type structures role responsibility, (3) the diverse ways in which blame is allocated to professionals, (4) the different communication problems that arise between professional employees and managers, and (5) the distinct ways in which these companies handle dissenting professional opinions. Our goal will be to describe how professionals can practice responsible computing in different corporate and organizational environments.

Finance-Driven Companies

1. Management and Professional Roles

In finance-driven companies, professional employees do not participate directly in the decision-making process. Instead managers make the decisions by (1) establishing goals, (2) soliciting and receiving information and options from professionals, and (3) synthesizing this into decisions that shape the day-to-day operations of the company. Professional employees fall outside the decision-making role. They participate, rather, as consultants who provide information, present managers with options, and answer questions.

2. Structuring Role Responsibility

Working with the frameworks we developed in the first section of this chapter, we will discuss finance-driven companies in terms of role responsibility and (in the next section) blame responsibility. In finance-driven companies, professionals are assigned the role responsibility of consulting. This gives rise to four obligations: (1) exercising **due care** when providing advice and services, (2) avoiding **conflicts of interests**, (4) maintaining **confidences**, and (3) remaining loyal to the legitimate interests and objectives of managers (**faithful agency**). The managerial role responsibility for decision-making is distinct from the professional's role responsibility of consulting. Consultants provide information and input to managers whose job, then, is to take this input, integrate it with other components (like financial considerations), and convert this raw material into policy and decisions.

The difficulty for computer professionals is that the obligations that professionals have as consultants do not exhaust their role responsibilities. Computing professionals also have obligations to the public as the following provisions in the ACM code of ethics indicate:

- General Moral Imperatives. As an ACM member, I will…
    - 1.1. Contribute to society and human well-being
    - 1.2. Avoid harm to others
    - "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."

In finance-driven companies, computing professionals often face situations where their responsibilities as consultants conflict with their responsibilities as professionals. (This,

again, follows from the fact that in finance-driven companies, ethical and professional values are not integrated into the financial values that form the company's central objectives.) Because professionals do not participate directly in the decision-making process, their options for promoting professional and ethical values are limited. They must persuade managers (the actual decision-makers) to attend to these issues in decision-making. Should this fail, then they must take on an oppositional role and search for means through which to manifest their dissenting views within the organization (a difficult process if the company has no formal means of recognizing dissenting professional opinions). If the dissent concerns important professional and ethical values, and management proves intransigent, then they must find ways of carrying out effective opposition. This can take two forms: **internal opposition** where professional employees use organizational politics (refs) to overrule a manager's unethical decision and **external opposition** where professional employees turn to such measures as whistle-blowing, i.e., publicizing the company's ethically questionable decisions and actions to the outside. Internal opposition can be exercised without breaking the bonds of loyalty with the company while external opposition breaks these.

3. Assigning Praise and Blame

The second sense of responsibility relevant in this context is blame-responsibility. How do finance-driven companies distribute praise when things go well and assign blame when they turn out badly? We see two distribution methods at work: (1) distributing praise and blame according to the position an individual occupies in the corporate hierarchy and (2) distributing praise and blame according to the social skills the employee has mastered. Position in the hierarchy determines allocation of praise and blame: praise moves up the corporate ladder to supervisors while blame moves down to subordinates. Social skills (the second consideration) can mitigate this *somewhat*. If an employee appears to be a "rising star" (or can attach to a rising star), then he or she receivers a greater share of the praise and more effectively deflects blame. Moreover, social skills help an employee to create the *appearance* of competence: effective office banter, dressing for success, and strategically cultivated friendships can compensate for lack of professional competence and low hierarchical position.

Because finance-driven corporations allocate praise and blame by corporate station and social skills, they do not adequately recognize and acknowledge hard work and skill. This injustice creates an environment that distorts somewhat the exercise of responsible computing. As we will see below, it pushes the responsible computing professional in the direction of blame-avoidance.

4. Communication Problems between Managers and Professional Employees

Communication problems arise when managers and professional employees withhold information from one another. (ref to Davis) The sharing of information between managers and professional employees is based on mutual trust which, in turn, is founded on the compatibility of the roles played by these two groups. The distinct roles managers and professional employees play in finance-driven companies can lead to one or both parties withholding information. Professional employees withhold bad news because they are afraid of being blamed for it. But because professional employees are among the

first to recognize ethical problems, their reluctance to bring these problems to management makes it less likely that these problems will be addressed early and effectively.

Managers also withhold information from professional employees for a variety of reasons grounded in the differences between these roles:

- *Managers are afraid that professional employees will subordinate their role as loyal employee to their role as professional.* As we saw above, professional employees have professional and ethical obligations that conflict with the financial goals of the company. Knowing this, managers will withhold information that could trigger a professional obligation and lead an employee to question or oppose financial objectives and management directives.
- *Managers assert and maintain authority over professional employees by controlling their access to information.* By breaking down a project into limited and discrete tasks and providing only the information an employee needs to carry out a limited task, a manager suppresses dissent and controls employees. Controlling information allows managers to take credit when things go well and pass off the blame when they don't.
- *Managers question the loyalty of their professional employees.* Professional employees change jobs and go to work for competitors. Hence, managers protect the company's confidential, proprietary information by withholding it.

Withholding information causes ethical problems because it delays and distorts effective response. Finance-driven companies are, as we have seen, especially vulnerable to these communication problems. Responsible professional computing requires designing strategies to work around these structural communication breakdowns.

5. Dealing with dissent

Finance-driven companies have difficulty recognizing and responding to dissenting professional views. First, managers restrict professionals to the consulting role; professionals provide information and answer questions but do not participate directly in the decision-making process. Managers brand professionals insubordinate and disloyal when they go beyond the consulting role and insist that their professional and ethical judgment be recognized in decisions. Managers also interpret attempts by professionals to participate more actively in decision-making as direct threats to their authority. Assertive professionals are branded "trouble makers"; they are told to become "team-players" or get out. Thus, professional employees who insist on raising dissenting views are subjected to reprisals that include poor performance reviews, exclusion from future projects, unwanted transfers, and dismissal.

Finance-driven companies often have policies on dissenting professional opinions that look good on paper. However, the implementation and enforcement of these policies breaks down because of the structural reasons we have enumerated (ref). Finance-driven companies take the priority of financial objectives for granted. Dissenting professional opinions challenge this by bringing competing professional and ethical issues into the

equation. Given these structural conditions, it is hardly a surprise that dissenting professional views are often treated with hostility.

6. Responsibility Program for Finance-Driven Companies
Finance-driven companies require a reactive approach to responsible computing that gives priority to staying out of trouble and avoiding blame. First, minimizing the scope or range of one's role responsibilities helps because the less one is responsible for, the less one is likely to be blamed when things go wrong. Professionals, in finance-driven companies, position themselves as consultants and, simultaneously, work to position others (managers) as the decision-makers who bear overall responsibility for the actions taken.

Second, this reactive responsibility stance precludes taking preventive measures. If a professional foresees an accident, he or she has the responsibility to notify the responsible decision-maker. But pushing further by, say, demanding corrective action, sets the professional up as insubordinate. So by notifying the decision-maker of the possible harm and *documenting* this notification, the professional has taken the necessary steps to stay out of trouble; if the decision-maker chooses not to act on this information, then the blame falls on him or her, not on the professional.

Third, the professional in a finance-driven company is aware that decision-makers tend to trade off ethical values for financial values. If the responsible computing professional is to make an effective case, say, for the ethical value of safety, he or she has to couch arguments for ethical and professional values in financial terms. One can do this by making them instrumental values that serve financial goals: safety and reliability are important because they improve company image and avoid expensive lawsuits.

Fourth, professionals who find it necessary to take an ethical stand against management, should expect a rocky road: (1) ethical dissent will be interpreted as insubordination and disloyalty; (2) the burden of proof will fall on the professional who will have to document positions thoroughly and completely; and (3) professionals should expect retaliation including attempts to discredit them personally. In general, responsible professional computing in finance-driven companies requires activating reactive, blame-avoidance strategies; if trouble is about to occur, they must warn decision-makers, document their concerns, and expect retaliation if they push any further.

7. Checklist for Finance-Driven Companies
Should you work for a finance-driven company? We (along with Jackall, ref) have presented a bleak view; yet there are benefits. Finance-driven companies are good places to work if management is ethically enlightened. Furthermore, an effective means to ethically enlightening these companies is for responsible professionals to work their way into management. The bad news is that the transition from professional consultant to manager is a difficult one; the good news is that many professionals can and do make this transition. What are some of the characteristics of those who practice responsible professional computing in finance-driven companies?

1. *Do you have strong social skills?* This would include the ability to discuss easily and naturally a broad range of topics, a sense of humor, the ability to gain trust quickly, charisma, the ability to blend in.
2. *Do you thrive in competitive environments?* Would you thrive in a competitive environment? Does competition bring out the best in you?
3. *Do you have what it takes to move into management?* Professionals who have managerial talents often find such a move rewarding. But managers need to be skilled in dealing with "people problems." They need to be able to delegate work and responsibility, work well under pressure, and be adept at making quick but accurate decisions. Some professionals successfully make this transition; others do not.

Quality-Driven and Customer-Driven Companies:
We now turn to customer/quality-driven companies. As we saw above, they can be treated as essentially the same when it comes to practicing responsible professional computing. Our source is the Hitachi report which shows that *Moral Mazes* provides only a partial portrait of the modern corporation. While Jackall (ref) effectively describes finance-driven companies, the Hitachi report provides a view of companies for whom the pursuit of non-financial values is not only a possible but a central aim.

1. Participation of managers and professional employees in decision-making
As we have seen above, professionals in finance-driven companies do not participate directly in decision-making. They influence the process only by working through those who do make the decisions, i.e., managers. They provide advice to managers, set forth options, and answer questions on technical matters within the area of their expertise. Should their professional or ethical judgment be overridden by a decision-maker, their recourse is limited to documenting their judgment; any further action constitutes opposition and violates the duty of faithful agency.

In quality/customer-driven companies, professional employees participate directly in the decision-making process. Decisions are made in interdisciplinary groups and emerge when group members reach a consensus. For this reason professional employees have a greater opportunity to build professional and ethical values into the organization's decisions. This greater participation makes it necessary to rethink the role responsibilities of professionals and to take a second look at the professionals role responsibility. The upshot of this rethinking, is that these kinds of organizations make it viable for responsible computing professionals to set aside blame-avoidance strategies and embrace a proactive model of responsibility as a virtue.

2. Structuring Role Responsibility
In customer/quality-driven companies, the functions of consulting and decision-making are not assigned to separate roles. Because of this, professionals incorporate both functions into their role; they become decision-makers *and* consultants when working on interdisciplinary work teams.

In customer-driven companies, because ethical and professional values are not necessarily integrated into the company's central objectives, professionals have the responsibility of advocating these values in the group-based, decision-making process. Managers in customer-driven companies have put this by saying that they expect professionals to "go to the mat" on professional and ethical issues; this means that professionals are responsible for ensuring that ethical and professional issues are adequately addressed in decision reached. In quality-driven companies, the need to advocate professional and ethical values diminishes because these are already essential components of the company's central objectives. The job of the professional is not so much to advocate these values as to provide creative, concrete options for realizing them. In short, professional employees in quality-driven companies are ethics **integrators** while in customer-driven companies they are ethics **advocates**.

3. Assigning Praise and Blame
Attributions of praise and blame fall primarily on the group and are related directly to results in customer/quality-driven companies; praise is connected to causal contribution and blame requires the presence of fault like negligence. Position in the hierarchy is no longer a crucial factor since the vertical hierarchy is often flattened out both within the group and between interdisciplinary, decision-making groups. Social skills are important but are transformed from those that make one stand out as a rising star to those that contribute to the group decision-making process; the latter include documenting one's position, communicating clearly, persuading/advocating skills, technical competence, articulateness, and integrity. Professionals are expected to remain committed to professional and ethical standards but to show creativity in integrating these with other values such as financial, technical, and manufacturing values. Group members share responsibility for good and bad results; distribution to individuals occurs only when a member performs in an outstandingly good or bad manner. In other words, group responsibility is distributed to individual group members based on causal contribution, competence, excellence, or (in situations where things turn out badly) the presence of moral fault.

4. Communication Problems between Managers and Professional Employees
Communication problems rarely arise in these companies for three reasons. First, professional and ethical considerations are well integrated into the central objectives of pursuing quality and fulfilling customer needs. Second, the integration of the functions of consulting and decision-making removes many of the motives that managers and professionals have in finance-driven companies for withholding information from one another. Third, because professionals participate in decision-making in customer/quality-driven companies, they find their work more satisfying. Hence, they are less likely to bolt to other companies, taking with them their former employer's proprietary information. So the motive for withholding proprietary information disappears in customer/quality-driven companies.

This is not to say that there are no communication problems in customer/quality-driven companies only that their character has changed. Participating effectively in work teams that produce decisions through a consensus process requires a different set of

communication skills. Professionals must be adept at communicating technical information in interdisciplinary terms. They must also master the art of rational persuasion, since the group consensus method requires recognizing and respecting the autonomy of the other team members. This, in turn, necessitates abandoning forceful modes of persuasion such as coercing, threatening, deceiving, and manipulating. Professionals, in this context, strive to become effective and creative value integrators (more on this below) and effective compromisers. So communication problems do arise in customer/quality-driven companies; but they are of a different nature because they arise from the complexity of group-based decision-making:

1. Failure to agree based on the need for more information (Solved by continuing the discussion and generating more information)
2. Failure to adequately integrate the different values put forth by group members (Solved by employing a design-based, value integration approach along with generating imaginative options)
3. Failure to communicate technical information clearly to an interdisciplinary audience (Solved by taking the time to explain one's position using concrete images, examples, and analogies)
4. Failure to make clear and persuasive arguments (Solved by practicing and developing skills of effective advocacy and avoid forceful or invasive means of persuasion)

5. Dealing with Dissent:
In quality/customer-driven companies, dissent is not polarizing; it does not divide groups into struggling factions. Rather it indicates that the decision-making process has not been completed. Thus dissent in quality/customer-driven companies is addressed, not by seeking to overcome or discredit one's foes, but by generating more discussion; this would include placing more/new information on the table, reexamining decision-making criteria, identifying and resolving conceptual muddles, and generating creative options, especially those that promise to integrate conflicting values. Decision-makers continue discussing the problem until disagreement is resolved and the decision made. If resources (time, money) run out, the best compromises are negotiated. While professionals are relied on by other decision-makers not to compromise on central professional and ethical values, they are expected to revise their positions when others provide good reasons for doing so.

The structural conditions that in finance-driven companies produce dissent (and make dissent difficult to resolve) disappear in quality/customer-driven companies. The manager/professional employee distinction is not so clearly pronounced. Professional employees are no longer asked to choose between professional and ethical standards and company loyalty since professional and ethical considerations have been integrated into the notions of quality and customer needs. Managers and professional employees no longer withhold information as a strategy to maintain control and as a defense against the arbitrary allocation of responsibility. Ethical problems are less likely to arise and are more quickly dealt with.

6. Responsibility Program for Customer/Quality-Driven Companies
The responsibility program we set forth above for finance-driven companies was a reactive, blame-avoidance strategy. This followed from the consulting role of the professional; because the professional does not participate directly in the decision-making process, he or she is relegated to documenting professional judgment when it is overruled by the decision maker. Since they cannot directly influence the decision, they are relegated to avoiding blame should things go wrong.

On the other hand, professionals participate directly in the decision-making process in customer/quality-driven companies. This allows for a proactive approach to professional computing. First, they can practice responsibility as a virtue which entails putting into practice all the characteristics we discussed above: defusing blame avoidance strategies, designing role-responsibilities with overlapping domains, extending the scope and depth of knowledge, extending control and power, and employing a design-based problem-solving approach. Second, instead of waiting for crises to emerge before responding, they can take aggressive and early measures to prevent problems as well as defuse disagreements. Third, their direct participation in the decision-making process along with the centrality of ethical and professional values in customer/quality-driven companies allows professionals to take a value integration approach to problem solving; instead of subordinating ethical and professional values to financial and technical values, they are free to explore (and generate) options that integrate these values. Fourth, professionals in customer/quality-driven companies can cultivate and practice the virtue of reasonableness (see chapter 3). In the context of group decision-making, reasonableness requires exploring value integrating options first, turning to compromises only when these prove ineffective, and taking up opposition only as a last resort. Finally, responsible computing in customer/quality-driven companies allows professionals to set aside blame avoidance strategies in the pursuit of more proactive measures.

7. Checklist for Quality- and Customer-Driven Companies
Interdisciplinary work groups form the locus of decision-making in these companies. Hence, those who will be successful are those who have dispositions conducive to this environment.

- *Collegiality*. Do you have the ability to get along with others, to collaborate with them, to share credit and blame, and to subordinate personal interest for group objectives?
- *Sharing responsibility*. Are you comfortable sharing responsibility for group results with other members of the group? (This would include identifying with the accomplishments of the group and taking pride in its accomplishments.) Are you willing to share work with others and pick up the slack when they fall short?
- *Strong Communication Skills*. (1) Can you communicate technical information in a comprehensive, concise, and intelligible form? (2) Can you disagree without making it personal? (Can you focus disagreement on issues and not on personalities?) (3) Can you understand positions with which you disagree? Can you use this understanding to identify common ground and basis for agreement?

(4) Can you clearly document your views and present them in an objective and dispassionate way?

- *Reasonableness*. (1) Are you willing to take the time to explain your views to others? (2) Can you answer their questions and concerns patiently and dispassionately? (3) Are you open to revising your own views if others present you good reasons for doing so? (4) Are you adept at resolving disagreements without resorting to force, deception, or manipulation? (5) Can you maintain a good, well thought-out, and well-grounded position, even in the face of pressure to abandon it? (6) Can you disagree with others and yet treat them respectfully?

These dispositions help bring about good group decision-making in quality- and customer-driven companies. They ensure discussions which issue in good decisions, rather than in rancorous disagreement.

Ethical Dissent:
Ethical dissent is not a single, heroic action. What begins with a single action (notifying an outsider of an objectionable behavior or policy) snowballs until it has absorbed inordinate amounts of the whistleblower's time and resources. It starts when an employee notices that things are not as they should be. Then the employee talks with people in the organization to attempt to change things. It can end easily, with changes made quickly, or it can end by involving an untold number of agencies, lawyers, legal systems, and public proceedings. Sometimes the whistleblower can control the course of events. Most often control dissipates as events unfold, and whistleblowers, who have acted only out of the best of motives, find their credibility attacked, their moral standing reduced, and their career trashed.

But ethical dissent need not go as far as making public allegations about wrongdoing in the company. It can involve as little as making a well supported suggestion that the policy be changed. Ethical dissent becomes whistleblowing when you make your dissent public by going outside the organization and contacting others to convince them to help you reform the organization.

The IEEE ethics committee has adopted a very useful set of guidelines for ethical dissent. Some of their recommendations are listed below in italics, with our annotations. The committee has provided its own annotations which are published at the online ethics site: http://onlineethics.org/codes/guidelines.html

1. *Establish a clear technical foundation*. Rarely can you prove your point with mathematical certainty. However you are much better off in making a complaint if you have done your homework carefully ahead of time. This guideline may not have helped Goodearl, since she did not have the technical background needed. But there were steps she could have taken, like making sure she knew the procedures and the exceptions in all their detail. She might then have proposed a solution that reconciled the need to get chips out the door quickly with the requirement that they follow testing guidelines.

2. *Keep your arguments on a high professional plane, as impersonal and objective as possible, avoiding extraneous issues and emotional outbursts*. If people become defensive they are unlikely to want to change. So your arguments should focus on procedure and product rather than people and personalities. In Goodearl's case, she clearly became branded as a "disgruntled employee" and this reduced her clout with Hughes and in the later court case.
3. *Try to catch problems early, and keep the argument at the lowest managerial level possible*. Advice about keeping things at the lowest level is similar to catching things early—they both minimize the magnitude of the change. Catching problems early is crucial. Once the product is already behind schedule or its delivery is publicly announced, it is hard to back away from the expectations others have developed. Sometimes, you might find it not worth making a fuss about the current product, and more worth your time to make sure that the problem does not come up again or is caught early on the next product.
4. *Before going out on a limb, make sure that the issue is sufficiently important*. By "going out on a limb" the committee here most clearly means whistleblowing: going outside the organization to report wrongdoing. Once this happens you will have burnt your bridges and will probably lose your job even if you are legally entitled to it. So it is important to weigh the costs of whistleblowing against its benefits. Are the costs to you, your coworkers and your employer worth the benefit of preventing harm or providing something good? Sometimes whistleblowing is the right thing, but the costs are almost always high.
5. *Use* (and help establish) *organizational dispute resolution mechanisms*. You should follow this bit of savvy advice **before** you get involved in a situation. Check **now** to find out if your organization has a dispute resolution mechanism. If it does not, work to establish one. It may help you later. It appears that Goodearl tried to use a dispute resolution process involving the personnel department but this failed when her contact there simply reported her complaint directly to her supervisor. If there had been a better designed dispute resolution process, her complaints might have had a fairer hearing. Don't get caught this way.
6. *Keep records and collect paper*. These should be kept beginning as soon as you realize that you might need to go either to internal dispute resolution or to the more extreme measure of whistleblowing. Reconstructed documents are not well received by others, since they depend on memory. When you begin to make a case for reform that you think might be resisted, document the process in as much detail as you can. You may need it later. Goodearl had some documentation in the form of a notebook she kept of her interactions. This notebook was crucial in the court case that followed her whistleblowing. But whether she had reconstructed some portions of the notebook became an issue in the case.

The running theme in the IEEE ethics committee's comments on all these issues is professionalism. Your complaint must be clearly laid out, without any personal bias, and argued on the basis of reason and not emotion. Don't get mad. Don't take it personally. Stay focused on the issues and avoid getting drawn into personal attacks. Base your dissent on *professional* judgment, that is, judgment that employs the same criteria and

exhibits the same level of competence as that of a reasonable and up-to-date professional in your field. Not all individuals in your profession have to agree with you; but all should recognize the seriousness of what you are doing.

These recommendations cover what to do *inside* your organization when you disagree, for ethical reasons, with some action your organization is taking. But at some point, it may become clear to you—as it became to Margaret Goodearl—that you will need to report the wrongdoing to someone *outside* the organization. This next stage merits further discussion.

Going Public: From Ethical Dissent to Whistleblowing

What if you have tried all the internal channels, and they have not resulted in an acceptable resolution of the issue? Perhaps you should go public with your allegations in order to put enough pressure on the organization to make the necessary changes. This is when it becomes "whistleblowing."

Things to think about before you blow the whistle

We provide a list of things you should consider before going public with your allegations of unethical conduct by an organization.

1. Make sure of your motivation.

Don't be led astray by motives of pride or revenge. *Do* concentrate on your duties to your organization, to society, and to yourself. Why do you feel the necessity to make your complaint public? What is the pressing need that must be solved? Here are some motives you might consider:

- *To show someone that you will not be ignored.* Often the process of ethical dissent within an organization is resisted by those who disagree with the dissenter or have reasons not to reform the organization's behavior or policies. If you have run up against this sort of resistance, you may feel motivated to "show them" that you are not a person to be trifled with. This motivation will likely lead you into trouble. It distracts you from actually fixing the behavior or policy of the organization. It also looks like retaliation for ill treatment because it readily leads to becoming a "disgruntled former employee."
- *To punish someone for their behavior toward you.* When we are injured by others, or when others thwart our reasonable desires towards reform in an organization, it is easy to get angry at those who stand in our way. But again, this motivation will distract you from your real goal, to change the behavior or policy of the organization. It will also make you an easy target for retaliation since it appears that you have a personal agenda in your whistleblowing. Hughes' lawyers at the civil trial attacked the credibility of Margaret Goodearl and her partner in the suit, Ruth Ibarra (Ruth Aldred by the time of the court hearings). But they failed to show that either had a personal vendetta against the company. Their behavior within the organization and their steadfast concentration on wrongdoing (rather than on wrongdoers) made this defense unavailable to Hughes.

- *To maintain your personal integrity*. If you feel you are being asked to engage in behavior that is unethical, you will likely want to distance yourself from it. But you may be able to distance yourself from unethical behavior or policy and maintain your own integrity without blowing the whistle. This motive may not require changing the behavior or policy of the organization; it may be satisfied by simply distancing yourself from the questionable behavior or policy.
- *To save your organization's reputation or finances*. It might seem paradoxical to make allegations public in order to save an organization's reputation. Nonetheless, there are occasions when this is reasonable and even necessary. If you have reason to believe that the organization will eventually get into trouble for their actions, then making the allegations public now may save the organization from greater damage later. If your goal is to change the behavior or policy of the organization so that it will be able to keep its reputation, you can still be a loyal employee while challenging the organization's questionable behavior or policy in public. In legislative circles, this is known as "loyal opposition." You would rather not play this role, but sometimes there is no other choice.
- *To reduce threats to public safety and health*. If you have strong reason to think that your organization's behavior or policy poses a threat to public health or safety, then you have uncovered a duty that may outweigh your duty of loyalty to your employer. The likelihood that the behavior or policy will threaten public health and safety (and the extent of this threat) constitutes the key factor in weighing these two duties.

The last two motives for whistleblowing show the cost of *not* going public. But there are also costs to you if you decide to go ahead and blow the whistle. We discuss these costs to help you reflect on going public.

2. Count Your Costs

If you intend to blow the whistle, plan to devote considerable time and trouble to proving your case. Outside agencies may show interest, but they are unlikely to believe unsubstantiated complaints. Unless you have the evidence to prove your allegations and are prepared to undergo intense scrutiny in terms of your motives and trustworthiness, you are not ready to go public.

In addition to these costs, you should also expect that your organization will retaliate against you when it finds out that you have blown the whistle. Organizations interpret whistleblowing as betrayal; they seek to punish whistleblowers to prevent others from exercising this option in the future. The statistics on the likely costs that whistleblowers will bear support this conclusion. These are taken from careful research done by Rothschild and Miethe (ref) who have interviewed or surveyed over 750 dissenters or whistleblowers. Their research indicates that organizational retaliation is both "severe and common." They document the following forms and rates of retaliation that occurred to people who dissented significantly *within* their company:

Form of Retaliation	
1) Lost their job or were forced to retire	69%
2) Received negative job performance evaluations	64%
3) Had work more closely monitored by supervisors	68%
4) Was criticized or avoided by coworkers	69%
5) Were blacklisted from getting another job in their field	64%

These forms of retaliation become 10% to 15% higher for those who go public, that is, go outside the company to blow the whistle. Also organizations retaliated more often against non-supervisors (vs. supervisors), African Americans (vs. whites), and whistleblowers who report about activities involving more than $100,000.

The outcomes of this retaliation can be severe for whistleblowers. The most common effects that Rothschild and Miethe (ref) document are:

Effects on Whistleblowers	
1) Severe depression or anxiety	84%
2) Feelings of isolation or powerlessness	84%
3) Distrust of others	78%
4) Declining physical health	69%
5) Severe financial decline	66%
6) Problems with family relations	53%

Those who dissent or who go further to blow the whistle rarely anticipate consequences this severe, but the research documents their frequency. But there is good news under all this bad news; in spite of the suffering they have endured, 90% of the dissenters and whistleblowers say they still would report the misconduct if they had a chance to do it all over. These individuals have come through the experience to see themselves as highly moral people who will do the right thing when it is called for.

Goodearl and Ibarra were harassed in their company, eventually released or fired, and spent a good deal of their time over the next decade fighting their case in the U.S. courts. They did not expect to have such a hard time proving their case and seeing things corrected. We have seen that the costs of whistleblowing exist and are well documented; those considering this option need to factor these costs into their decision to go public.

While you think through your intention to blow the whistle, you should be clear about the costs you and your family may suffer if you blow the whistle. These decisions are not easy, but they may be—as was the case with Goodearl and Ibarra—matters of life and death for others.

When to Blow the Whistle

Richard DeGeorge (ref) presents a checklist for when whistleblowing is morally permissible (when one has the right but not the obligation to blow the whistle) and when it is morally obligatory (when one not only has the right but the obligation to blow the whistle). His analysis integrates the reversibility test with the harm/beneficence test.

From a deontological standpoint, it identifies the duties that usually conflict in these situations: the duty of confidentiality to the organization vs. the duty professionals have to safeguard the safety, health, and welfare of the public. Moreover, it sets up a general utilitarian analysis where the costs of not going public (exposing others to harm) are weighed against the costs to the organization, the whistleblower and coworkers of violating confidentiality. The result is a checklist with five steps:

A. Three conditions must be satisfied if whistleblowing is to be morally permissible:

1. *Serious and Considerable Harm.* Concerned professionals should resort to whistleblowing only to avoid serious and considerable harm. Professional codes of ethics recommend notifying proper authorities to avoid harm to the safety, health, and welfare of the public. The ACM code for computing professionals explicitly mentions whistleblowing as an option. But whistleblowing has its costs as we have seen above. It is justifiable only if these costs are outweighed by the harms the act of whistleblowing is designed to prevent.
2. *Notification of immediate supervisor.* Whistleblowing is not a first resort but a last resort. Employees have the responsibility to give their supervisors every chance to respond to and correct the questionable behavior or policy. If the supervisor is responsive, this provides the best (and least harmful) resolution of the problem.
3. *Exhaust internal channels before going external.* When the immediate supervisor fails to respond adequately, the whistle blower should seek out and inform other individuals within the organization of the problem. The concerned employee, again, should give the organization every chance to respond to and correct the problem. DeGeorge recommends exhausting internal channels up to and including the Board of Directors. In many situations this may not be possible; there may not be enough time to do this and prevent the harm. If Goodearl and Ibarra had tried to do this, they would have been fired long before they reached the Board of Directors. Consequently, many have interpreted this as requiring that one pursue internal resolution through two or three more levels of supervisor before going outside. Hence, this condition is better understood as making a reasonable effort to bring the problem before different individuals within the organization to give the organization several opportunities to respond to the problem before taking it outside.

B. With the addition of the following two conditions, whistleblowing becomes a duty:

1. *Documented evidence.* We discuss this in more detail below. Documented evidence should be sufficient to convince an impartial and objective observer of the seriousness of one's claims.
2. *Likelihood of successful resolution.* Whistleblowing brings about harms as well as benefits. It should be undertaken only when there is a high probability that going public will solve the problem that motivated whistleblowing in the first place: changing the questionable behavior or policy and preventing the serious and considerable harm.

DeGeorge's five conditions do not give us a mechanical procedure for determining when to blow the whistle. But they do raise the key issues. Blowing the whistle is a last resort that we save only for serious and considerable harms. We must give the organization

with the questionable behavior or policy the opportunities to correct the problem. Whistleblowing allegations must be backed with documented evidence that would convince an impartial observer. Finally, since the costs of blowing the whistle are high, the results should be worth the trouble, i.e., that the harm is averted by being brought to public attention.

3. Obtain all the necessary background materials and evidence.
There are two purposes for the background material and evidence that you will be collecting: documenting the wrongdoing and protecting yourself. You should keep a notebook (and regular backup copies, even of paper material) that catalogues your evidence and provides the context for it. You should date everything you obtain and date the notes you take. Do not do anything illegal to obtain your documentation, but do be creative about the forms of documentation that you get as well as with ways they can interlink.

Written evidence and supporting documentation are crucial. You should record all the dates and times when events related to your case occur, when you receive or obtain documents, and when you consult with others. If other employees are present when these events occur, record their names so they can back up your story. When recording events, stay as close to the facts as you can, without drawing inferences about motivations that people might have. What did they say? (*Not* why did they say it or what is their underlying motivation?) What happened?

If the company tries to fire you or asks you to resign because of specific problems, you will need to document that you are doing your job well and that there were no complaints lodged against you prior to your dissenting or whistleblowing. Obtain a copy of your past performance records. Did your appraisal scores drop as soon as you made the wrongdoing a matter of public record? Companies sometime "restructure" in the wake of whistleblowing, and this can be a form of retaliation. Be sure that you have evidence that the company structure is stable before you go public, so you can show the relationship of the restructuring to your whistleblowing and dismissal.

4. Organize to Protect Your Own Interests
A protection system is much more complex than just written documentation that you are correct in blowing the whistle. Your family and close friends can provide support when things start to get difficult around the office. But you must weigh this support against the importance of minimizing the people who know the details of your case. You need to involve your family and friends as outside sources of support but withhold from them confidential details.

After mustering all the documentary evidence you can, and making sure you have support from friends and family, consult a lawyer about the paths you can take as a whistleblower. Both case law and government statutes are constantly changing. Consulting a legal professional, particularly one familiar with your local whistleblowing laws, is your best bet to protect yourself. Laws covering the public and private sector in

the U.S. differ in the remedies and protections they offer whistleblowers. Laws outside the U.S. may provide either more or less coverage than U.S. or state laws.

5. Choose the Right Avenue for Your Disclosure
So, your case is ready, you have legal counsel, and you have family support. To whom do you make your disclosure? All your potential allies in this action will have mixed motives, many of which will not agree with yours. You should carefully analyze your options before you step out into the public with your allegations.

Regardless of the avenue of disclosure you choose, you should plan to reveal only the information you need to make your case. This must be negotiated with your disclosure partner. Take care to protect your own confidentiality and that of the organization you work for. Make your disclosure in such a way that you minimize the disruption and damage to your organization. Remember, information is your main resource in whistleblowing; once you release it, you lose control.

Here are some risks and benefits associated with disclosing to different parties:

1. *Government Agencies*. Some governmental agencies have hotlines for whistleblowers. Since they were working for a private company that had a contract with the military, Goodearl and Ibarra made their disclosures to the Office of the Inspector General for the U.S. Military. Legal counsel can help you in deciding if there is such a special reporting agency for your circumstances. Government agencies certainly oversee a great deal of business in the United States, and this oversight varies from country to country. These agencies can often be the most effective allies in your campaign. But you should be aware that they may have interests that conflict with your disclosure. Again, legal counsel can help you in thinking this through.
2. *Judicial Systems*. State and federal district attorneys are often the appropriate pathway of disclosure for illegal activity. But they have their own reasons for picking up or ignoring a case such as case load, the need to find cases to set case law, and ambition. You will need someone who knows the layout of the land to advise you here.
3. *Legislators*. Often local, state, or federal legislators can help you find your way to the right people to make a disclosure to. They also have the resources to investigate the improprieties themselves. Again, they have their own motives. For example, elected officials can place their concerns about maintaining cordial relations with their constituencies and donors over your concerns and interests.
4. *Advocacy Groups*. Advocacy groups may be able to give you good advice about who else would be a good medium for disclosure. Often, though, they are not themselves in the position to investigate your concerns or to pressure organizations to change questionable behaviors or policies.
5. *News Media*. New media may give you a quick way to make your allegations public. But they lose attention quickly. They will not provide sustained pressure unless your case continues to be newsworthy during the long months that you attempt to pursue it.

6. Make Your Disclosure in the Right Spirit
"Duties of loyalty and professional ethics require that employees make their disclosures in a manner that minimizes the damage to their organizations." (ref) You have a duty of confidentiality to your employer regarding trade secrets and proprietary information. Disclosure of detailed confidential information may subject you to legal liability. Disclose your information only to the extent necessary and only to authorities who expressly agree to keep confidential information confidential.

If you become publicly identified as a "disgruntled former employee" who is out to cause maximum damage to your former employer, then you will also lose leverage as an honest broker of important information. Remember, your job is to change the behavior or policy of the organization while causing as little disruption as possible.

Movies and Whistleblowing
While movies have a tendency to sharpen conflicts for dramatic effect, they do present some of the existential aspects of whistleblowing, i.e., the difficulty of making decisions under pressure, the loneliness of whistleblower, ways in which organizations put pressure on whistleblowers, and other negative effects of whistleblowing. Some of the movies that we like:

The Insider: The costs of whistleblowing are nicely dramatized as we watch Wigans lose his job, family, and self-respect. He also finds himself subjected to character attacks and finds himself contemplating going to jail because his whistleblowing involves violating a confidentiality agreement. This movie also provides a nice analysis of the difficulties and risks associated with using the media as a vehicle of going public; the media has its own interests that can turn against the whistleblower.

Silkwood: This movie does a nice job of creating the moment of decision where Silkwood finally decides to go public. It also provides a fascinating character sketch of a person who is willing to face all kinds of obstacles to challenge questionable organization practices.

Civil Action: Civil Action dramatizes the difficulties employees of Grace and Beatrice had in going public and testifying to illegal disposal of toxic materials. It also shows how legal action can spin out of control and produce results that don't accord with our moral perceptions.

Class Action: This is an older movie that refers to two, possibly three, whistleblowing events. First, there is a whistleblower who committed suicide when he felt abandoned by those who encouraged him to go public. Second, there is the drama of a lawyer trying to decide what to do when she discovers that evidence has been illegally destroyed to cover up wrongdoing and incompetence. Finally, we see how even knowledgeable professionals can look ridiculous when they fail to present documentation and convincing arguments to support their claims.

Erin Brokavich: This movie culminates when a shy employee of Pacific Electric finally comes forward with documented evidence of illegal disposal of toxic wastes, the so-called "smoking gun." It provides an opportunity to reflect on the difficulties of identifying a suitable source to whom to blow the whistle and the importance of mutual trust in successfully resolving the problem.

Quiz Show: This movie may not at first seem to shed light on whistleblowing. But it shows how one can be caught up in a cover-up and how difficult it is to go public in these situations. Charles VanDoren's final confession shows how agonizing it is to break out of a cover-up, admit to wrongdoing, and face inconsistent public reaction.

There are more examples. Whistleblowing makes for good drama and movies have done a good job of showing how it feels to be involved in this activitity, how real its costs can be, and still how important it is to keep one's integrity throughout.

Guidelines for Designing an Ethical Dissent Process

Process for supporting ethical dissent in organizations go by many names: open door policies, appeals policies, grievance policies, ethical dissent procedures, dispute resolution procedures, etc. We provide here some guidelines on what an effective, comprehensive procedure should do. Many of these assume a fairly large organization with extensive personnel resources. Smaller organizations and shops cannot afford these extensive support mechanisms, and may be more likely to adopt relatively informal "open door" policies. These recommendations are taken from an extensive literature that is summarized in (ref).

An ideal ethical dissent procedure should provide:

- *Integration of existing advocacy groups*. If the procedure does not include unions or professional groups in the process, it will be perceived as (and may actually be) an attempt to cut those legitimate interest groups out of the decision review process.
- *Clear reporting procedures and contacts*. The people who should be contacted and the procedures for contacting them should be clear, and there should be clearly specified consequences if those persons ignore complaints.
- *Written complaints and replies*. Open door policies are less likely to adopt these, but in larger organizations, complaints and replies should be documented. This protects all parties and provides a trail of responsibility for review. It also focuses discussion on the complaints and the arguments rather than on personal dynamics in face-to-face meetings.
- *Reasonable deadlines for submission and review*. It often takes longer than one might imagine to put together a persuasive case that a policy should be changed. Adequate time should be allowed. In addition, most complaints can be de facto effectively denied if the response can be delayed long enough.
- *Investigation by non-interested party*. If possible, someone who is not the defender of the policy or decision should be the investigator. This person is unlikely to be entirely non-interested (they do, after all, work for the company).

But the are obvious reasons why it is difficult for a boss to be the one to review complaints about his or her own decisions.

- *Use of a panel for complex or difficult cases*. In a larger organization, complex decision can require the expertise of a panel of professionals and managers. This also provides the opportunity to look for a consensus outcome.
- *Regular review of the procedures*. Data should be collected about the outcomes of the procedures, and the procedures themselves should be reviewed periodically to see if there is an pattern of bias in the procedures.

In an ideal ethical dissent procedure, the initiator should receive:

- *Guarantees of confidentiality & non-reprisal*. If the organization wants to encourage ethical dissent, then it cannot punish those who use the procedure. Often these guarantees involve a promise of transfer to another work group of branch of the organization.
- *Support for making and pursuing case*. People who use these procedure are unlikely to be familiar with the process. They will need support in navigating the procedures and in making a persuasive case. An ideal procedure provides that support.
- *Regular updates about progress in investigation*. When a complaint has been initiated, the initiator should be kept up to date about how the process is going, the stage of investigation, and be allowed to supplement the case as needed during its review.

In an ideal ethical dissent procedure, outcome should include

- *Explicit links to disciplinary proceedings*. If in fact people are at fault, there should be a requirement for disciplinary action. Otherwise a report can simply languish while the unethical decision goes unchallenged.
- *Explicit links to policy review and change procedures*. Again, simply producing a report is often a way organization use to avoid actually taking action. People responsible for policies should be required to respond in a timely fashion to a report and to show that they have taken the report into account in their policy or decision change.
- *Guidelines for external reporting*. There should be guidelines for what data about outcomes and process are publicly reported in the organization, and that data should be archived for later access.