The Failure of Information Ethics

John Orlando, Norwich University

Just about every human activity raises ethical dilemmas. There are medical ethics, business ethics, environmental ethics, journalistic ethics, and even sexual ethics. So it shouldn't come as a surprise that new developments in information technology, such as the Internet, have spawned ethical dilemmas as well.

Investigators are just now feeling their way into the new information ethics issues. But because the field is in its infancy, there is no agreement on how to approach these issues. Thus, commentators to date have been concerned with identifying a method for solving information ethics issues. This has meant generating systems of rules that are supposed to solve the ethical conundrums. These rules are like decision machines; the user is supposed to input the relevant considerations of an ethical dilemma into the system, and out will pop the answer. The commentators are reaching back to their undergraduate ethics days, where they learned the grand systems of Immanual Kant and John Stuart Mill, to develop their own grand systems of information ethics[1].

Unfortunately, these systems are of almost no help in solving any interesting ethical dilemmas. The problem is that the rules advanced by commentators are too general to point in any particular direction when faced with all but the most obvious situations. The data goes in, but no answer comes out. The ethical decision machines simply cannot handle real life dilemmas.

The fundamental problem is not so much that the decision machines these commentators give us are faulty, but rather that rule-guided ethical reasoning by its nature typically underdetermines the outcome in interesting cases. Even the theories of Mill and Kant provide us with little if any help in addressing practical issues like abortion. It's always painful to watch an undergraduate student doing a presentation on abortion make the mistake of asking "what would Kant say about abortion". The inference gap between theory and practical issues is so great that the student is soon adrift; left drawing conclusions that have no basis in the principles from which they are supposedly derived.

Information ethics commentators fail to understand that most people do not solve ethical issues by the application of foundational rules. Ethical

[1] Kant, Immanual. *Grounding for the Metaphysics of Morals* (J. W. Ellington trans.), Indianapolis: Hackett Publishing, 1993.
Mill, John Stuart. *Utilitarianism*. Indianapolis: Hackett Publishing, 2001.

rules, including the grand historical theories, are better used to explain deep-rooted moral intuitions than guide reasoning. That is, they are used as a way of understanding the nature of ethics, not as a practical means of addressing ethical issues.

My goal here is to demonstrate the failure of information ethics principles by showing how the ones advanced to date fail to help us solve real life information ethics dilemmas. I will do so by looking at what these principles can say about two sample information ethics issues. I will then demonstrate how an entirely different, non-rule based, and in fact more common, approach leads to insight where information ethics principles are silent.

Public Records on the Internet

The first issue concerns access to public records. As Chey Cobb recounts:

> [A] few years ago in the state of Florida, the legislature passed a bill encouraging counties to make their public records available online, via the Internet. One result is global access to deeply personal data that people assumed would only ever be seen by someone who made an effort to go to the courthouse and request a copy.
>
> Apparently nobody in the Florida legislature realized that what they had done was make it easy for members of the Russian mafia to find the names, addresses, and social security numbers of elderly Florida residents who have given power of attorney to their children. And how many legislators were encouraged to vote for that bill by donations from high tech companies who stood to gain juicy contracts for computerization of public records?[2]

We can extrapolate a couple of ethical questions from this case. Should government entities be allowed to put public records on the Internet? Alternatively, should government entities be required to put public records on the Internet?

Information Warfare

The second issue concerns information warfare. In recent years information systems have not only become a target of war, but a weapon of war. There is reason to believe that the United States, and possibly other countries, has developed computer viruses to be unleashed on an opposing side's computer systems during a conflict. Even if the weapons have yet to be developed, technology allows them to be developed, and so it makes sense to question whether their use raises ethical problems.

To provide some flesh to the question, consider the following scenario. Taiwan makes good on a longstanding threat to declare formal independence from mainland China. China responds by initiating a war with Taiwan. As part of the hostilities, China launches a series of computer viruses against Taiwan's information systems. The viruses attack the military, economic and medical structures of Taiwan, resulting a massive

[2] See Chey Cobb's unpublished work "Ethics and High Technology," prepared for the Norwich University Master of Science in Information Assurance program, Seminar 4, Week 3, 2003.

downgrading of Taiwan's ability to defend itself. Because of this, Taiwan surrenders. The question is: Was China's use of a computer virus as a weapon unethical?

Computer Ethics Systems

Now that we have a couple of interesting information ethics issues let's take a look at how the information ethics systems to date would handle them.

The Ten Commandments of Computer Ethics

Perhaps the best known information ethics system is the "Ten Commandments of Computer Ethics," which states:

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.[3]

While these rules may sound lofty, a closer examination proves that they are unhelpful in solving either of our ethical dilemmas. Concerning the case of public records on the Internet, we must keep in mind that the issue is not whether the Russian Mafia acted wrongly. There is no disagreement that it acted wrongly. The issue concerns the actions of the Florida Legislature. Should the government have put public records on the Internet? The government is not violating any of the Ten Commandments listed above: it's not using a computer to harm other people, to appropriate other's work, to bear false witness, or do anything forbidden by the rules. You can't claim that it ignored the social consequences of its actions (rule 9) or did not respect others (rule 10). It enacted the law precisely because of the social consequences of its actions, to make it easier for citizens to access the information, and out of respect for its citizens.

So nothing in the action violates the Ten Commandments of Computer Ethics. But a lot of people would still think that there is an issue. Why? Because there are a lot of considerations not addressed by the Ten Commandments of Computer Ethics. In fact, none of the relevant considerations—such as the likely use of the information by others, or the right to have that information—is addressed by these rules. The rules are simply not equipped to address the relevant considerations.

[3] Chey Cobb, op. cit.

We encounter the same problem with the case of computer viruses as weapons of war. The act does not violate the rule against bearing false witness, or any of the like. Since a computer virus causes harm, you could say that their use as a weapon of war violates commandment 1. But it makes no sense to discount them on this ground because all weapons cause harm. Commandment 1 does not say why it's impermissible to cause harm with a computer rather than any other weapon.

Commandments 9 and 10 are unhelpful because they're so vague in their own right to point in no particular direction with this issue. Are the social consequences of using computer viruses as a weapon of war good or bad? They're good for your side and bad for the other. Similarly, are you showing consideration and respect towards your fellow humans by doing so? Winning the war is showing consideration for the people you are representing but not those on the other side. But this is what war is all about. The rules are not equipped, nor intended, to challenge the concepts of just war, and so are not helpful in this matter.

Blended Rules System

James Landon Linderman provides another set of rules for solving information ethics dilemmas. These are three basically independent rules that he says will guide us to right behavior concerning computer use:

1. The Golden Rule (Do unto others as you would have them do unto you).
2. Consideration of the interplay of duties, rights and responsibilities remains important.
3. Traditional reasons for good ethical behavior, such as religious principles, egoism, utilitarianism, and altruism still provide us with a useful taxonomy for discussions about ethics.[4]

Once again, we find that when it comes time to actually apply these rules, they provide little guidance. For instance, did the Florida legislature violate the Golden Rule in asking municipalities to put public information on the Internet? If a state senator votes for a bill, she presumably would have no problem with any one else voting for the bill as well. This is true of any bill, and so The Golden Rule is unhelpful in guiding her decisions. Again, it can tell us that the Russian Mafia acted wrongly in ripping off elderly residents with the information, but this is not an issue. The issue concerns the actions of government, and whether public information should be put on the Internet.

Rule number 2 tells us nothing more than consider all of the relevant information. But who would assert that one ought not to consider all of the relevant information? In fact, the statement borders on a tautology because "relevant information" could be defined as "that which should be considered." So it tells us that we should consider everything that should be considered. Rule #3 just shunts the work off to traditional ethical rules, and Linderman conspicuously tells us nothing about these other rules or how they would solve any interesting issue.

[4] Both Linderman references are from "Ethical Decision Making and High Technology," *Computer Security Handbook*, Fourth edition, (Wiley: New York, 2002), ed. Bosworth and Kabay, Ch. 30.3.2.

Later, Linderman adds three more tests meant to guide ethical deliberation:

1. The "mom test" asks how your mom ....would react if aware of your actions.
2. The "eye-team" test takes this a step further and considers the results of exposing your actions to the whole world as part of an investigative team broadcast.
3. The "market test" asks you to think about openly publicizing your actions as a competitive customer relations strategy. (30.3.3)

In essence, each rule tests for the same outcome. It asks if making your actions public would cause embarrassment, and if so, then the action is wrong. Essentially, it assumes that the person applying the test has an innate sense of right and wrong, and would only act wrongly under the cover of secrecy. Someone who steals generally knows that stealing is wrong, but does it because he puts self-interest above ethics.

This works well with obvious cases, such as stealing, and with people who are predisposed to be ethical, but it doesn't work to solve interesting questions, ones where there is reasonable disagreement about the proper course of action. Someone who believes that the use of computer viruses as a weapon of war is morally permissible has no problem telling his or her mom about it, or anyone else for that matter. Similarly, the legislator who votes for the law requiring public records to be placed on the Internet is not going to be guided by a test of publicity because all of his or her votes are public. There's no question of secrecy in this arena.

Kantian System

Mich Kabay provides a Kantian guide for addressing information ethics decisions. He tells us to ask two questions:

1. Does your idea show respect for other people or does it treat them as tools for your own gain? Would you feel "used" if someone did what you are thinking about to you?
2. And what if everyone acted as you suggest would that be good or bad in general? It's like walking across the grass in a pretty garden instead of taking a couple of extra steps to stay on the path: if you're the only one doing it, it may not hurt the grass. But if everyone did it, soon there'd be a muddy path across the corner instead of the grass.[5]

Once again, these rules are unhelpful in answering either of the issues above. The question of whether China is showing respect by using a computer virus as a weapon of

[5] Mich Kabay, "Making Ethical Decisions: A Guide for Kids (and Parents and Teachers too)" (2001) http://www2.norwich.edu/mkabay/ethics/making_ethical_decisions.htm
These are variations of Immanuel Kant's well-known first two versions of the Categorical Imperative: The Principle of Humanity and the Principle of Universalization.

war is no different from asking if the use of any weapon in war shows respect. This can only get us into theoretical speculation about just war and pacifism. The real question is whether computer viruses are a uniquely unethical weapon of war. Answering this question requires comparing them to other weapons.

We run into a similar outcome when trying to apply rule number 2 to the situation. What if everyone uses computer viruses as a weapon of war? Presumably, the world would be worse off, but this is true of any weapon. So this consideration can only lead to general critiques of the rightfulness of war, which is not the issue. Similarly, it makes no sense for the Florida Legislature to ask if it would "feel used" if someone did to it what its doing now—which is voting on a new law. If a State Senator thinks a law is a good idea and votes for it, she would have no problem with others voting for it as well. The question is whether it's a good law in the first place.

How we do ethics

Instead of applying moral rules, we normally use what I call "the method of analogy" to solve moral issues.[6] Basically, we determine the moral status of the case in question by drawing an analogy to a case where the moral status is clear. The idea is that if we can agree about the moral status of act X, that it is morally right or wrong, and that act Y is relevantly similar to act X—meaning that there is no morally relevant difference between act X and act Y--then we are compelled to apply the same judgment to act Y. This draws on the principle of consistency in reasoning; that the judgment applied to a case must also apply to all relevantly similar cases. Without that principle, reasoning is not possible.

We appeal to this method all the time. If I see my son stealing another child's toy, I might try to convince him that his actions are wrong by asking if it would be wrong for that other child to steal my son's toy. If my son agrees that the other child's actions are wrong, and that "there is no difference" between his act and the other child's, then his act is wrong as well. Even very young children understand this principle intuitively.

Moreover, it is often easy to find cases, real or hypothetical, where there is widespread agreement on its ethical status. Everyone agrees that hacking into a computer system to retrieve credit card numbers for personal gain is wrong. If the act under question can be shown to be relevantly similar to this act, then widespread agreement can be generated about the ethical status of the act under question.

Public Information on the Internet

Now let's see how the method of analogy, instead of appeal to the information ethics systems, can be used to examine the two ethical dilemmas I raise starting with public information on the Internet. The most important point in examining this case is that records in question are already available for public viewing. All one needs to do is go down to the courthouse, or city hall, and request them. In fact, it's likely the case that these records must be made available to the public. That is, given that the records are

[6] This method is outlined in *The Abuse of Casuistry: A History of Moral Reasoning*, Alber R. Jonsen and Stephen E. Toulman, (Berkeley: University of California Press, 1988).

public, it would probably be illegal for the Florida legislature to prevent public viewing of the records in question. Nobody is arguing that the records should be hidden, so there is widespread agreement that the current situation is ethically permissible.

The Florida case involved municipal records such as property values and taxes, as well as court cases, all of which are available for viewing to anyone willing to stop off at the courthouse during business hours. There are legitimate uses for these records. Appraisers use property records to compare a particular property to similar properties that were recently sold. An individual might also want to know if his own house is being over appraised, and thus he is paying too much in property taxes (which can only be done by comparing the appraisals for different properties), or if the Mayor's own property is suspiciously under appraised. Certainly it is critical that court records remain public to prevent the morally egregious secret trails that one finds in despotic regimes. Landlords also check court records to see if potential tenants have been forcefully removed by court order in the past.

So we are currently in a situation where these records are available to any citizen willing to go to the local courthouse or city hall to view them, and there is widespread agreement that these records should be available to the public. Moving the records online only makes it more convenient for citizens to exercise a freedom already available to them. There is no difference *in kind* between the two situations, only a difference *in degree*, the degree of convenience in access the records. There is no morally relevant difference between the current situation and the one where these same records are put on the Internet, and so the action is not morally wrong.

One could even go so far as to argue that the government is *obligated* to put the records on the Internet because it would make them accessible to those who would not otherwise be able to reach them, such as people in a nursing home or others who are homebound. Those who are homebound do not have the public access available to those who are not so unfortunate. My guess is that it would be illegal to store those records in a place that is not handicapped accessible. Similarly, those unable to leave the home at all are unable to access records not on the Internet. Of course the government might not be obligated to go to all lengths to provide maximum convenience for all of its citizens, but it might be obligated to increase assess ability to public information when the cost is not prohibitive, as in this case. Moreover, court and property records are often publicized in newspapers or other media sources, which is not significantly different from the Internet either.

The fact that improving the convenience of access also improves the convenience of crime is just a regrettable cost of living in a society with an open government. Nothing has been done to make possible a crime that was not possible before. The Russian mafia could always access the information used in the crimes, it is just easier to do it when it's online. Also, the information itself is not sufficient for the crime. Criminals have to take the information and misrepresent themselves to con people out of their money.

This case demonstrates how information ethics systems handcuff ethical deliberation by tracking it into considerations that are not relevant and ignoring those that are. The major

consideration here was that the public records are just that, public, meaning currently accessible. None of the systems mentioned earlier will allow us to input this important information into the formula, and so none can handle the issue. The result is that contemporary issues are often examined in artificial isolation from alternatives. Applying the theories forces us to ignore relevant considerations.

Viruses as a Weapon of War

Turning to the use of computer viruses as a weapon of war, let's see if we can find an analogy between computer viruses and some other weapon for which there is widespread ethical agreement. One strong possibility is biological weapons. After all, the very term "computer virus" borrows its name from a biological virus. It's not hard to see why. Like a biological virus, computer viruses spread indiscriminately. A computer virus might only affect certain types of hardware or software, such as a Microsoft server, but it does not distinguish between civilian and military servers, hospital, school, or government servers of this type.

Here I think we've gotten to the heart of the ethical issue concerning computer viruses as a tool of war. Conventional weapons cause fairly well defined harm; a missile that hits a building can be predicted to cause a certain amount of damage to that building, and anyone in it, but not more. But the reach of a computer virus is unpredictable. Self-replicating code will move indiscriminately between systems, limited only by the type of system with the vulnerability it can exploit. Computer viruses could destroy medical information, causing hospital deaths to civilians or other non-combatants not targeted by the viruses. Moreover, a computer virus does not stop producing harm when the other side surrenders; it does not know if a truce has been called.

This unpredictable and indiscriminant nature is certainly at the heart of our moral intuitions against the use of biological weapons. Soldiers exposed to biological viruses could carry them back to their families or community. We abhor biological weapons over conventional weapons much because of their unpredictable targeting, and computer viruses share this nature.

Another way to see this is to look at people's moral reactive attitudes--feelings of anger or resentment--towards people that release computer viruses on the Internet. These viruses only directly attack machines or information on machines. Yet people's anger towards these virus writers is at least as strong, and not stronger, than their anger towards people who commit a more direct harm, like theft of a car. Why this extra bit of moral anger towards virus writers? I believe it can only be explained by the fact that virus writers tap into a deep-seated anger towards those who cause indiscriminant harm, like vandalism. The lack of focus to a particular harm, a clear and controlled target, adds to the moral wrongness of an act in our minds. Biological weapons and computer viruses share this indiscriminate nature.

One might object that unlike biological viruses, computer viruses do not infect people, they infect machines, and so their harm to people is only indirect. But while this is the case, is it a morally relevant difference? Imagine that a country developed biological

weapons that also did not directly attack people, but rather destroyed crops in order to cause mass starvation. Or imagine that a country released a bacterium that ate critical resources, such as oil (which are actually being developed to combat oil spills) or water? My intuition is that such weapons would be treated as morally contentious. This means that biological weapons that cause harm only indirectly are still morally questionable. The analogy to computer viruses still holds.

Conclusion

People have come to recognize that computer use, like all areas of human activity, raises ethical issues. This has generated a literature on information ethics. So far, that literature has been concerned with developing ethical systems—modeled on the rule-based systems of the past—to address the new ethical issues. The belief is that without a common foundation of information ethics principles, we cannot make ethical judgments about computer use. Unfortunately, these rules do more to put an intellectual cramp on moral reasoning than lead to enlightenment. We are able to examine the new information ethics conundrums using the method of analogy common to everyday moral reasoning.

In reality, the information ethics rules that have emerged are best used as guides for children who are first encountering the power of computers. Interesting problems, the ones that produce widespread disagreement, demand a much higher form of thought to solve. I don't claim that my examinations to two sample ethical issues are the last word on the subject. I fully expect, and even hope, that others take these examinations further. My point is only to demonstrate a methodology for addressing the issues we are sure to encounter as information technology continues to bring us to new frontiers.