INFORMATION SYSTEMS: ETHICS AS TAUGHT AND PRACTICED

In Information Systems, the introductory course textbook typically has a chapter at the end of the book which discusses topics in ethics and information systems. As I would go over these concepts with the students, they seemed "obviously true", but somehow not realistic. In advanced courses, while discussing current capabilities of systems, I became more aware that what we teach as ethical behavior at the introductory level in information systems is not always consistent with what is (or must be) practiced by information systems professionals and the capabilities of the systems they oversee. This paper is an attempt to uncover some of those inconsistencies as a first step toward generating an ethic which can be accepted at all levels of information systems.

Before we begin looking at ethical issues, let's review what an Information System is and its use to a company. Laudon and Laudon [1] define an Information System as:

> a set of interrelated components working together to collect, retrieve, process, store, and disseminate information for the purpose of facilitating planning, control, coordination, analysis, and decision making in business and other organizations.

A number of studies [Atkins [2]; Yasin and Quigley[3]] have surveyed companies asking about the central role and purpose of Information Systems. The typical answers were that IS should increase market share and reduce costs, or that information systems should provide a strategic competitive advantage.

That is, the focus is collecting data and using it in some way that enables your firm to make more money.

I. Privacy

The first topic I would like to look at is privacy: with respect to customers, with respect to employees, and with respect to the world. Privacy encompasses many topics: data collection, monitoring, security, hacking (getting into files you shouldn't).

What do we tell our students about privacy of data?

We need to protect the confidentiality and privacy of data. Data should not be collected for one purpose and then used for another. We should minimize data collected, limit access to data, provide security for data and dispose properly of data after a given retention period has passed. Persons have the right to know when data is being collected about them.

What are we doing with respect to customers and privacy?

We are amassing databases that capture incredible amounts of information about which the customer is probably not aware. Cordell [4] argues that, when integrated into one large database, these databases may deprive individuals of their privacy.

Nicholas Negroponte [5] states "All of a sudden, our smallest actions leave digital trails...Blockbuster, American Express, and your local telephone company can suddenly pool their bits in a few keystrokes and learn a great deal about you...Each credit-card

cards through (you can track how long employees are in any given area) [13];

there are proximity readers that can vet your ID cards up to 8 feet away [14];

biometric devices that can scan your retina, the length of your fingers, and your weight to make sure an impostor hasn't taken your place [15];

revolving door "mantraps" equipped with metal detectors [16];

e-mail letter openers and keystroke-monitoring programs have become so routine that any manager who purchases network operating software is getting built-in snoop features [17];

Gamecop is a software package that monitors PCs to see if any Windows games are running. You have the choice to display a customizable message telling the employee to get back to work, or it can sound an alarm and embarrass the user in front of his/her co-workers [18];

at Xerox PARC in Palo Alto, Ca, workers wear badges (2"x2"x1/4") that emit a unique signal so the computer system knows where any given employee is at all times. The badges are intended as tools to help staffers locate their friends. The creator Roy Want, a computer engineer, states "The benefits to be had are so great; we just have to be sure that the people who are in control respect our privacy." [19];

22% of business leaders admitted to searching employee voicemail, computer files, and email. Macworld estimated in 1993 that 20 million Americans were subject to electronic monitoring through their computers on the job [20];

By late spring, the message management specification will be published. It will all dynamic monitoring of messages: allowing the network administrator to trace the path of a message even if it goes across multiple platforms and to see the status of every component on the messaging network [21];

Network Event Recording Device is an automated, real-time system for monitoring and detecting network anomalies (developed at Los Alamos Nat. Lab) NERD triggers an alarm when any suspicious behavior occurs on the network. Shadoware uses artificial intelligence to compare users' current use patterns with prior, presumed normal, activities. It maintains a "digital fingerprint" of each user based on 38 usage variables [22];

Why have information systems managers and network administrators become so involved with monitoring of employees?

Computer theft is becoming the significant crime of the 90's. $1 Billion worth of computers were stolen in 1993, only 7% were recovered. One large bank, which loses on the average one computer a day, also loses 300Mbytes of bank information every day [23];

One recent survey [24] finds that fraud is often an inside job and that:

41% of IS employees would illegally copy software,

7% of IS workers would adjust a bank account system to avoid incurring a service charge, and

10% saw nothing wrong with writing a virus program to output "Have a Nice Day";

Another study [25] found that 80 to 90 percent of business theft is internal,

58% of misappropriation of information involves insiders, and

because of employee resentment in downsizing, computer-data trashing is on the

charge, each supermarket checkout, and each postal delivery can be added to the equation. Extrapolate this trend and, sooner or later, you are but an approximation of your own computer model." By the way, what did that agreement you signed when you got your Jewel card say? "I authorize Jewel-Osco and their data processing supplier to utilize information about the products I purchase" [6].

EShop software [7] allows retailers to simulate their shops with 3-D views of navigable aisles on the Internet. Three stores who opened in February 1995 are 800-FLOWERS, Tower Records and Land's End. It provides detailed customer tracking and profiling data that allow retailers to target customers for specialized promotions. "It'll tell us if a customer lingered over an item but didn't buy it. The next time that person enters our online store, the personal shopping assistant can offer the same item to that customer for 10% off and maybe close the sale" says the manager of 800-FLOWERS [7].

The government is a large information systems employer. Beginning in 1996, the IRS will have direct, online access to your pay records, banking and checking histories, stock transactions, extra income, outstanding loans, credit-card debts, trust disbursements, motor-vehicle records, and deductible business expenses. Their plan is that you may not need to file your income taxes. IRS will do them for you and send you the bill [8].

A bill passed recently encompasses mandatory wiretap standards for every telecommunications carrier in the US with a fine of $10,000 per day for services that aren't wiretap ready [9].

Paradice [10] expresses the attitude about privacy this way: There are "conflicting assumptions made by computer systems users and computer systems professionals. While users assume they have total privacy regarding their computer work, computer professionals assume they have total access to anything in the system."

And the near future for customers?

George Colony is president of Forrester Research, an organization that predicts future trends. He believes the future will see lots of dedicated devices, small and free. For example, Domino's might give you a device with two buttons: pizza with cheese, pizza with pepperoni. By simply pressing one of these buttons, a pizza will be delivered to your door in 15 minutes. You may also see a trash can scanner. As you throw products into the trash, a signal is sent and the next day, a refill on the discarded product is delivered to your door [11].

Pattie Maes, a professor at MIT, is working on software agents. These agents learn about a user's habits, interests and behaviors with respect to some task they do frequently (such as looking for certain topics on their network). They detect patterns and then automate them on behalf of the user. Agents will also be able to share with other agents what they have learned about their respective users. How long until these are in use? Maes predicts 2 years [12].

What are we doing with respect to employees and their privacy?

We are monitoring their every move.

Is computer monitoring an invasion of privacy?

Let's look at some of the types of security being used:

digital smart-card keys remember which gateways employees have swiped their

rise.

Thus, security is a serious consideration to many IS managers. So serious that any methods seem justified in keeping data secure. Sherizen [26] finds that senior executives have become corporate information police without wanting this responsibility, understanding what it means, or knowing what to do with it. The message must be given to senior executives that they no longer have a choice about implementing information security. Courts and regulatory bodies could hold them [managers] responsible if someone inside the company commits a technology-related crime [27].

What are we doing with respect to the World and privacy?

1. Increasing monitoring capabilities worldwide.
2. The Internet is replacing government regulations.

Inslaw is a Washington D.C. based company which made a database management software called PROMIS which allows US agencies, primarily the CIA, to surf the computers of foreign banks and spy services thru a "backdoor" [28].

The Internet is seeing 1 million new users per month. NSFNet, keepers of the net.backbone in the U.S. say that new foreign networks connected to the Internet will soon outpace those connecting from the US [29].

Attack scanners are software designed to probe networks worldwide looking for security holes. An attack scanner known as SATAN (Security Analysis Tool for Auditing Networks) is scheduled to become available on the Internet to any and all takers next month [30]. This certainly can be classified as hacking software, though it is justified by IS managers as a type of software needed to run on their own systems to look for security holes. A current estimate of the amount of time it takes for any type of software to become available to both "the good guys and the bad guys" is 2 months [31].

The pressure of world-wide networking means that we are no longer able to set rules which apply only withing the USA and expect them to be enforcable. DigitalLiberty is an advocacy group dedicated to the principled defense of freedom in cyberspace. Its purpose is to construct new global communities and render the government irrelevant. Bill Frezza, in their mission statement, says "DigitaLiberty does not seek to educate or influence politicians in the hope of obtaining legislation favorable to our constituents. We plan to make politicians and legislators irrelevant to the future of network-based commerce, education, leisure and social intercourse [32, 33].

The Illusion of Privacy

David Brin [34] believes that privacy is just an illusion. He asks a simple question "Do you honestly think that any privacy law is going to keep high officials, like George Bush, or billionaires, like H. Ross Perot, from finding out anything and everything they want to know about you? No privacy act will ever prevent the rich and powerful from snooping about you. All such laws accomplish is to prevent *you* from finding out about *them*."

Perhaps we have reached the point where the capabilities of software (which are certainly being used by IS managers) have made privacy, as we teach it, incompatible

with privacy as we practice it. We should look for a new formulation of this concept.

II. Software Reliability

What do we tell our students about software reliability?

It is unethical to release software with bugs, which has not been fully tested. Software should do what it promises and it is unethical to misrepresent the capabilities of software.

What are we doing with respect to software reliability?

We are using creating buggy software, using buggy software and waiting for customer or user complaints to work on problems.

Possibly the largest and most well known software creator is Microsoft. Their successes as a business are studied in many business courses. They are well-known for bug-filled late releases. A survey in February by Computerworld [35] found that 61% of IS managers "did not trust Microsoft to deliver products without bugs. The same percent said this did not affect their willingness to use Microsoft software". Microsoft makes a database management system called Access. Several large companies complained that Access randomly corrupts data. It was hoped that release 2.0 would fix it, but it didn't.

What is the lesson that we learn from Microsoft's success? That you must wow your audience, bugs don't matter so much if you promise to try and fix them in the next version.

David Parnas, an engineer who worked on SDI says that it is impossible to produce bug-free software [36, 37]. The mathematical functions that describe the behavior of these [software] systems are not continuous functions and traditional engineering mathemathics does not help in their verification. Since the number of states in software systems is so great, we cannot check them all, thus there will always be errors we have not found. If Parnas is correct, we are setting our students up for 'ethical failure' on their first big system project.

A further worry in software reliability is the use of expert systems for decision making. Specialists who construct these programs are focused on the correct way to capture an expert's decisions in a series of if-then statements; the focus is not (and cannot be) on whether or not the expert is correct. Should we be asking about the values of the expert? Computerworld, [38], reports the use of an expert system used in mortgage decisions. Using their expert systems, mortgage lenders are able to instantly approve a buyer's credit and eliminate the need for certain traditional documentation. One Va. firm can complete a buyer's credit check in less than four seconds.

Issue: an expert system is made by patterning ONE expert's methods of problem solving. If this expert is biased (as we all are) against some group (women, minorities, disabled, etc.) then many more cases of discrimination can occur and this will be a "computer decision", not a human decision. We are representing computer decisions as unbiased when then may not be. Not very much is known about how persons who have created these systems make ethical decisions or how information which comes out of these systems influences ethical decision-making behavior [39].

Forester [40] suggests that analysts who design computerized systems are not completely powerless because they have more opportunity to influence decisions than those merely affected by the change but not involved in its design. The analysts have

access to information and can control certain agendas. Moreover,analysts can leverage their power to mediate distorting influences by anticipating the effects of power and conflict.

III. Minor point of irony

We say:

Viruses are bad. Don't even think about putting one on a system. Viruses can be as destructive to a computer system as an abortion is to a fetus.

We do:

Honor the creator of computer viruses. A recent issue of Computerworld [41] announced (not an ad) a talk of interest to IS managers. It is to be given by the inventor of the first computer virus, Frederick Cohen, and focuses on computer security. Why did he create it? He developed the first virus for his Ph.D. The cost of the seminar includes a copy of his book.

Can you imagine a group of right-to-lifers attending a talk by the creator of the abortion pill?

IV. Summary

In an interview about non-lethal weapons research currently underway at Los Alamos, the researcher explained [42], "This is a classic area in which the technology is outstripping ethics and philosophy...We no longer have the time to have decades of debate."

The same is true of Information Systems. We are so driven by the rapid demands of the marketplace that these are shaping what we do.