# CONSCIENCE IN COMPUTING, A LAW DAY PERSPECTIVE ON COMPUTER CRIME

Jay BloomBecker
2700 N. Cahuenga Blvd.
Los Angeles, CA 90068

---

I want to tell you how important it is that you and I together think about what it means to us, and to all of society, to think about computer crime. There are real costs to you and me, and there is a real role that you and I can play, changing what happens in the next two, five, twenty-five, twenty-five-hundred years. We are so sublimely fortunate to be living at a critical turning point in our society. The decisions that we make are going to be far-ranging, perhaps more than the decisions of anyone before us. So you see, I am a true fanatic: believer in the importance of computers for the future of our society. I'm almost a little guilty to tell you how true this is. Because, when I was in college, I started reading about computers, which for a liberal arts student who knew he was going to be a lawyer from the age of five, was almost unheard of. Why read about computers if you're going to be a lawyer, people said to me. And what I didn't say as often as I might have was: "That's where the money's going to be. That's where the power's going to be. That's what's going to determine who controls the world."

For that reason, I am as convinced as I could possibly be, that thinking about something as abstract and frankly economically insignificant as computer crime, is about as challenging an undertaking as there could possibly be. For that reason, to talk about computer crime on Law Day is a double challenge, because we have all these amazing social changes taking place in our society, focusing on the role that the computer plays in our life. And on Law Day, I have the rare opportunity to see where the law fits in.

On Law Day, we celebrate life in a nation of laws, and not of caprice. How many times have you heard that, or something like it, before? How many speakers, at this very moment, on campuses across the United States, in luncheons across the United States, are saying the same thing? Well, for me, the sentiments have a peculiar importance.

Tomorrow, I will go into New York City and go to a Consulate, attempting to get a visa to go to a European country that shall remain nameless. I want to visit a book fair in this country, and I have been negotiating a visa for the last six weeks. And when I asked the General Counsul what the rules were to determine whether I would get a visa or not, he said he didn't know. As I say, I hesitate to name the country. I fear it would interfere with my attempt.

Now, without being so optimistic as to think that a similar nightmare might not be set in the American bureaucracy, I think that on Law Day we celebrate the large amount of space in which our's is a nation of laws, and decisions of our national policy are made fairly and rationally, rather than arbitrarily. In a nation of laws, I have been brought up to believe that the law protects the oppressed, and gives security to the righteous. The challenge I face is the question of whether these high sentiments have meaning when we talk about computer crime.

Do computers oppress us? Or, more precisely, do the people who use computers, or the ideas we have about computers, oppress us? Many students of computing suggest that computers can be the tools of oppression, and of oppression far more pervasive than anything we have experienced thus far. The specter of 1984 haunting us for forty years, is ironically dominant in these remaining months of 1983. Five calendars are coming out on the market, dealing with computers (which says a lot of other things about how we view computers). But, two of those calendars focus on the Orwellian implications of 1984.

Consider the computerized bracelets now in limited experimental use in Albuquerque, New Mexico. The bracelet sends a signal to a microprocessor. The microprocessor, kind of a combination computer and transmitting station, receives a signal. It is attached to a telephone. If someone wearing the bracelet goes more than 300 feet from the telephone, the telephone automatically calls the police department computer and steps can be taken to punish the person who is wearing the bracelet. Is this progress, allowing prisoners to stay home rather than to spend time in jail? Or is it oppression? "Will it mean that we start to use computers to keep people under constant surveillance because they've had a traffic ticket?" asked one ACLU representative quoted recently.

If it is oppression, do we need new rights to protect us from the oppression of the machine? Is this a place for criminal law? When we contemplate the scope and the purposes of computer crime law, such questions are hardly academic.

How do computers relate to our security? Security in general seems in short supply in our time -- whether it is security from attack in the street or security against nuclear annihilation. It should come as no surprise then, that computer

security is a novel development in a still-novel field.

Computer Insecurity, the title of a recent book by Adrian Norman, in England, seems to be growing far more rapidly than computer security, as daily more and more of us find ourselves forced to confront a computer-dominated future, whether we are ready for it or not. I hesitate to plunge into computer crime, fearful that you may dismiss me as a Luddite, one of those English machine-breakers of the 18th Century, in lawyer's clothing. To speak ill of computers seems contrary to the only segment of the national economy that seems to offer the prospect and the promise of dramatic growth in the foreseeable future.

I don't want to break the machines. I don't want to stay the revolution. I just want to point out that the role of law is not limited to anticipating newer and more lucrative distribution packages for "Pac Man" video games. It's not limited to urging sensible taxation of software, or fashioning reasonable copyright protections for those whose genius fuels the computer revolution. The role of law, and the role of citizenship, in a modern cybernetic society, is to put conscience in computing.

Conscience. That's what we're about when we talk about computer crime. Conscience, or the lack thereof on the part of the criminal. But also, conscience, or the lack thereof, on the part of our computerized society. There's trouble ahead and computer crime is just the most visible and the most dramatic aspect of it. As we lawyers try to fashion laws to confront the problems arising from computer crime, I think we can do ourselves, our profession, and our society great service if we are able at some time to infer more general insights about how we are to deal with the various oppressions and insecurities that may accompany the computerization of our society. For, at its heart, the computer society will succeed or fail based on the belief on the part of all those in that society, that the use of computers is fair. Fair to them. That it helps them more than it hurts them. In short, to repeat, that there is conscience in computing.

Let me just point out the fact that much of the conversation about computer crime has a jovial ring to it. I will make many comments this afternoon that may well elicit laughter. I hope so. It tends to make me happier when you laugh, and please, feel free. And yet, as I say that and as I look back over other speeches that I've given, I always have a fear that people will come up to me afterwards and say, "When you laugh about computer crime, you are encouraging it. You're supporting those people who think computer crime isn't such a bad thing." And, we ask, why doesn't conscience keep everyone from thinking computer crime is a bad thing? And one answer is, many people don't think the victims of computer crime are going to hurt much. And they don't feel particularly sympathetic to them. It's not like people are being hurt, after all.

But, isn't that odd? Doesn't that at some level demonstrate how little faith we have in the computerized society? Far too often for my comfort, computer crime is seen as the way in which those people who are the "outs" can take revenge on those people, or those machines, who seem to be on the ins. And if we really thought that those machines were serving us, and representing our investment of our assets into our society, then it would be no more tolerable to hear about a machine being damaged, than to hear about any other creation that people put time and love into being damaged. And if we heard about $1-million being lost by a bank, we wouldn't say, "Oh, they probably stole it from the poor people like us anyway", we'd say "Gee, a bunch of innocent stockholders are going to get less money this year." So as we talk about what computer crime is, I think it's important to keep in mind that what we're really talking about is what computers are and what our society says we're willing to do to defend those new-fangled things called computers, that we seem to have put so much faith and so much money into.

Well, what is computer crime? Depending on who you are, very different definitions of computer crime will appear congenial to you.

If you are a journalist, computer crime is an ingenious, almost baffling feat of technical mastery of man over machine, preferably involving the loss of over $1-million. (If you write for Cosmo or Ms., I should add that it would probably be a baffling feat of technical mastery of woman over machine.) Last week, when a programmer stole $7,000 worth of Los Angeles Dodger tickets, newspapers called him a genius. My computer friends pooh-poohed and said no genius gets caught that quickly. More important, no genius would be satisfied with $7,000. They suggested the case may signify a significant change in what we should call the national pastime.

And that's another story that the newspapers are beginning to pick up, that "don't trust anyone under 15" may become the watchword of computer conservatism, as we worry about the ability of those younger than us to out compute the rest of us. At the same time, as I say, different groups define computer crime very differently. If you are a computer manufacturer, computer crime is a misnomer to begin with. It makes no more sense than filing cabinet crime. Thus, it's not surprising, I suggest, to find IBM taking out two-page color ads in Time, Fortune, and similar magazines, to tell the world, "The Computer Didn't Do It", and to show a terminal in a line-up with four other people, highlighting what IBM is doing on behalf of computer security. As the leader of the field, this is no inconsiderable amount. But, it seems that you can sell more newspapers with computer crime than you can to sell computers.

I don't make these observations from an omniscient perch on Mount Olympus, or even in impartial perch in Lake Placid. I, too, define computer crime to sell something. I sell law enforcement.

The National Center for Computer Crime Data, works primarily to give information to law enforcement agencies and other groups that want to fight computer crime. And the broader we view computer crime, the more effort, I believe, we can put into dealing with the large variety of crimes that are of concern in our society.

I believe that computer crime should be defined in the way that offers society the greatest security against oppression by computer use or computer abuse. Conceptually, I think my definition is quite simple. Computer system crime is any crime involving inappropriate interference with rights or other assets resulting from computer system use. More and more, computer system use creates new social assets, the potential for new rights. Some assets are obvious. As we computerize businesses, groups and individuals buy computer systems. And the law normally protects property rights in such tangible items as computers, printers, communication lines, data processing centers, microprocessors, chips, floppy diskettes, printouts and the like. How well it protects these tangibles is another question.

A computer system processes information, an intangible entity, as different from solid machines as dreams are from coal. No business person who has used computers long, can escape recognizing the value of intangible assets resulting from computer use. Application programs calculate the most economical bill payment practices, they control production of a company's biggest selling item, they speed the creation of perfect documents. But what are these application programs?

They're bunches of electronic blips on a magnetic medium, a disk, a tape, a diskette. You can't see them, you can't feel them, and traditionally the law hasn't known what to do about them. You can copy these electronic blips in a minute or less without harming the original. And here the law has difficulty in providing even the definitions necessary to protect the property involved.

Consider this example. A Denver investigation company decided they could perform a valuable service by "borrowing" medical records of personal injury plaintiffs, and selling that information to the defendants. They hired a couple of nurses who would order records using their doctor's names, and then deliver them over to the company which would copy the file and return the originals to the nurses. The investigators were caught, prosecuted, and let go. Information itself cannot be stolen, said the Supreme Court in Colorado. These men never intended to deprive the doctors of the files, just to steal the information on them. And information itself cannot be taken.

When a programmer in California stole a program from a competitor of his employer's, the court found him guilty of theft of trade secrets, but it suggested that he might have gotten off if he had taken the information alone.

And application programs aren't the only kind of information resulting from computer use. There are other types of programs: operating systems, utilities, and the like. There are also data bases, collections of information of considerable value to those who invest in their creation. That's why thieves in Denmark stole a Reader's Digest mailing list and here in the U.S., stole a "Diner's Club" list. It should be obvious that the person, or business, who pays to create tangible property like programs or data bases, has a right to secure use of that property.

But what about the subject of the data base? You or me? What rights have we if someone gets information about us? Let's say someone looks in my credit file and sees the numbers from my credit cards, and gets a bunch of swanky magazines, the kind that allow you to buy things through the mail using just your credit card number, and he sends for a bunch of gifts to himself, typing all the applications on a public typewriter so no one could trace who sent the items. And there is my credit card number for him to get a new lounger, or a personal computer, or a subscription to The New Republic. This happened in Northern California and there was little legal protection available to Mr. Alan Kahn, the person whose credit card was used. The fellow receiving the goods bought on Mr. Kahn's credit card, played it cool when he was questioned. "People just seem to like me and send me things. I don't know why," he said. We have been debating privacy in the computer age since the mid '60s, and a clear articulation of these rights to privacy remains to be achieved.

Moving onto another kind of computer crime, with the computer comes computer services, or computer time, another intangible type of property. Here in New York, a programmer was prosecuted for theft of services because he used the Board of Education computer for his own resume and for some horse-breeding information. He was not, contrary to news reports, handicapping horses. He was found not guilty, when the court ruled that New York's theft-of-services law did not apply. A couple of bills introduced in your legislature would presumably cover this offense.

One of the major services performed by computers is accounting for the various assets that a company, or an individual, possesses. And many of the most dramatic computer crimes have involved alteration of the computer's functioning so that money, or other assets, represented in the computer or guarded by the computer, could be stolen. The accuracy and the reliability of the computer is itself the asset compromised in cases like these. In the Wells Fargo case, $21.3-million was diverted into various accounts controlled by Harold Rossfields Smith. An accomplice simply kept the bank's computer from sounding an alarm while the money was flowing to Smith's accounts.

Finally, there is another category of computer assets, perhaps most intangible of all. This is a

set of expectations that computer use can be trusted to do a job better than non-computer methods. I call this expectation "the computer's good name". The examples of abuses of this kind of computer asset are many. Computer dating services offer young people like you the opportunity to meet members of the opposite sex, or in these more liberated times, the same sex, with the assistance of a computer. And in some cases that have been prosecuted, there has been no computer, which is worse than proving that there's no Santa Claus. In other cases, there were computerized horoscopes, so called, where the computer performed functions limited to sorting cards and typing labels. Now we in the modern world think that love and astrology are never susceptible to science, but like to pretend that economics is. And thus we would put in a different category the schemes whereby investment crooks promised 200% interest on investments because they used computers to outsmart the rest of the investors, either in the options market or in another similar investment scheme. In two such cases that have been prosecuted, there was a theft of over $50-million.

There are many questions to be answered before this list is complete. What privacy rights should be recognized as worthy of criminal protection? What rights against deceptive practices in the sale of computers should we assert? What rights against intentional misuse of computers that bill people? What rights, perhaps, against gross negligence in setting up of computer systems, causing economic or physical injury to people?

Law will doubtless define various rights of computer users and others in response to growing consensus about what rights require protection in our time. But when? After how many abuses? People sometimes ask me what the difference is between the National Center for Computer Crime Data, my organization, and Stanford Research Institute, a Northern California organization of much greater age and resources. I like to say the difference is that Donn Parker says he would hate to be called the Ralph Nader of the computer industry. I could think of no greater achievement.

What should we do about these computer crimes? As I suggested before, defining the crime is not the whole problem. Our laws prohibit many of those computer crimes I've listed. Nineteen states already have computer crimes law right now. Many of them prohibit many of the same acts that state laws already prohibit. The approach of these laws in my opinion, neither fully grapples with the problems inherent in defining computer crime, nor is responsive to the needs expressed by those people most involved in fighting computer crime.

We can use law to redefine criminal behavior, to cover more computer crime -- and I hope we will.

We can also use it to make investigation and prosecution more certain, and punishment more severe.

We can also use computer crime law to try to set standards for computer security and to reward those who meet these standards, and punish those who do not. At the outset, our law needs to consider the numerous intanglible assets that computing creates and make sure they are adequately protected. For starters, this requires a thorough reading of every state's penal code, to see all the places referring to property, and making sure that all the fruits of computing fit within these definitions.

To improve the criminal justice system will require, however, much, much more. Should we make use of a computer in the commission of a crime an enhancement, like using a gun? Consider the use of computers by the inmates at the Framingham prison, who were accused of using it for drug distribution, gambling, and other illicit purposes. Should we outlaw the use of programs like locksmith, that are used to defeat software protection and permit illegal copying of copyrighted software? We have the analogy of burglary tools. Are there cybernetic age burglary tools we should prohibit, or license?

So many questions to ask. Should we facilitate prosecution for theft of microprocessor chips by making it a crime to remove or alter company logos on those chips? Do we need more creative sentencing options for white-collar computer criminals? These are just some of the questions that would go into an analysis of perhaps what might be called computer crime procedure laws. In practice, these laws are passed or not passed at the same time as other computer crime laws are passed.

Likewise, a whole field of opportunity presents itself when we consider the fact that most computer crime never comes to the attention of law enforcement. Some European laws make it an administrative misdemeanor to operate a computer center lacking adequate security. Some American laws offer civil immunity to those who report computer crimes. But these are just two of many possibilities. What other laws could make detection of crime more likely? What laws could move victims to use the criminal justice system more? Do we need, for instance, special streamlined procedures for the trial of computer crime cases? Special departments of the court to handle all high-technology matters? Departments where the judge is most certain to know the law applying to computer property, or admissability of computerized evidence?

I raise these questions not because I have the answers. Just because I believe an intelligent discussion of computer crime requires their consideration. If you try now just to remember the six categories of computer crime I have mentioned, you can see the enormity of the problem law faces trying only to deal with this one aspect of computing. Only one of the new technologies that are becoming part of our lives. Similar questions will present themselves about the limits of man/machine interaction. Do we want machines acting as psychologists? As lawyers? As public speakers? What about the rules for computer-based decision making?

A while ago, "redlining" was challenged as unfair to minorities. What other kinds of decisions are made based on some mathematical formula that may not be fair? Think of the troubles we have with redistricting, and so forth, and so on.

What are the ethics that we want to enforce in the business field, where computers are concerned? As computing progresses then, our challenge is this, as lawyers, as citizens, as participants in the Information Revolution: we must ask of each innovation, not only what are its benefits, but what are its costs? What are its oppressions? And what insecurities will it bring with it?

Hopefully we can then answer what are the symbols, the legal concepts, the institutional structures, that can provide the security our society needs to accept the benefits of these technological advances.

There is a confidence implicit in Law Day. For over 200 years, our nation has dealt with its problems through the vehicle of law. We can be confident, I suggest, that the "can-do" spirit that has brought our nation this far, is nowhere more evident than in our current technological leadership. So, too, can we guide our technological future under the rule of law. So, too, can we put conscience in computing.