

FIFTH GENERATION COMPUTER CRIME LAW

By Jay BloomBecker
4053 JFK Library - California State University
5151 State University Drive LA CA 900320

Director, National Center for Computer Crime Data

ABSTRACT

As the "shock absorber" of social change, criminal law will serve to deal with the most troublesome results of the progress in artificial intelligence and expert systems research and applications. We will have to redefine crimes against the person, property, public morality, and the public order. To do this will require considerable change in our standards of culpability, computer performance, and the functions of punishment.

Introduction: Why bother with computer crime law?

1. Good social programming anticipates worst case scenarios

If computers, communications, and their many social manifestations are seen as the vehicles of "progress," computer crime law may well be seen as a "shock absorber" with which society tries to avoid the greatest disruptions along the way.

As so thoroughly and insightfully noted in Langdon Winner's Autonomous Technology, the fear of present and future technological change is already a considerable reality. From Frankenstein to WarGames a ready market has existed for those works of fiction suggesting that the development of technology holds dangers as well as promises. In a rational world, the law of computer crime would be designed to provide the best tools possible to minimize these dangers.

2. The law must be goosed

Anyone reviewing the 37 state computer crime laws collected in the National Center for Computer Crime Data's Computer Crime Law Reporter might easily harbor doubts as to the laws' rationality. Couch argues that the laws' focus is seldom on those areas in which law enforcement personnel report the greatest need for help. Seven years of debate have failed to dislodge any

substantive computer crime legislation from the U. S. Congress. Perhaps a look at the problems of tomorrow will conduce towards convincing the potentially politically powerful partisan of progress in computing that his or her help is needed by those politicians in power today.

3. Progress is not inevitable in any generation, not even the fifth.

Bruce Nussbaum, writing in The World After Oil, summarizes his fairly straightforward extrapolation of current computer criminality thus: "The crimes of the 80's and 90's will increasingly involve the theft of high technology through tapping electronic transmissions. People, companies, and the government itself will be both victim and perpetrator." [at 223]

More globally, Professor Winner argues that our current view of the computer "revolution" is based on what he calls "mythinformation," which he defines as "the almost religious conviction that a widespread adoption of computers and communication systems and broad access to electronic information will automatically produce a better world for humanity."

["Mythinformation in the high-tech era," IEEE Spectrum June 1984, at 91.]

Computer crime law can play an important role in shaping the future of the computer revolution. It can serve to communicate and create computer security for all of us.

4. Computer crime law is a good mental isometric

Thinking seriously about computer crime requires thinking seriously about our values, an invaluable exercise in an age as devoid of moral consensus as the computer age seems to be.

A. What shall the strategy of a fifth generation computer crime law be?

Criminal law is not created in a vacuum. Bassouni acknowledges that criminal law operates as an instrument of social control: "it employs strategies of coercion to obtain certain goals. That postulate is predicated upon the assumption that society having made a value judgment on the significance of certain interests it seeks to protect and preserve resorts to coercion to achieve its essential goals ." [Substantive Criminal Law p. 77.]

Consider the following expressions of the values embodied in criminal law:

The American Law Institute Model Penal Code defines the general purposes of provisions defining criminal offenses thus:

"To forbid and prevent conduct that unjustifiably and inexcusably inflicts or threatens substantial harm to individual and public interests"

The Yugoslavian Criminal Code reflects both similarities and differences:

"This Code protects from violence, arbitrary treatment, economic exploitation and other socially dangerous acts, the person of citizens, their rights and freedoms..."

1. What interests shall computer crime law protect?

A fairly standard categorization of the interests protected by the criminal law lists crimes against persons; property; public morality; and the public order.

In predicting the tasks of fifth generation computer crime law we must consider what new rights and assets will arise in a decade or two of computer breakthroughs, and which of these will require the protection afforded by criminal law.

1a. Crimes against the person

The most serious crime against the person is homicide. A man was crushed to death by the operation of an industrial robot in a Kawasaki factory near Kobe Japan in 1981. [New York Times Dec. 13, 1981 Section 3, p. 27, col. 1]

In fiction, a woman died when a utility mistakenly turned off her heat [Intruder by Louis Charbonneau]

Professor Gemignani asks: "Could

'Hal,' the computer of the film 2001 be tried for murder? How about Hal's systems programmer or his builder?" [Product Liability and Software 31 Defense Law Journal (1982) at 335, 368]

While those questions lurk, ask yourself whether invasion of privacy qualifies as an "invasion of personal security" deserving the protection of criminal law proscribing crimes against the person.

Hints of future answers to these questions have recently surfaced in two of the more progressive computer crime laws enacted in Virginia and Connecticut.

Section 18.2-152.7 of the Code of Virginia defines "Personal Trespass by Computer" to cover use of a computer without authority "with the intent to cause physical injury to an individual" [Computer Crime Law Reporter I-73; also see Connecticut Public Act 84-206 Section 5, enhancing punishments for computer crimes in which the perpetrator recklessly engaged in conduct which created a risk of serious physical injury to another person. Computer Crime Law Reporter I-10]

Section 18.2-152.5 of the Code of Virginia criminalizes "Computer invasion of privacy." [Computer Crime Law Reporter I-73]

1b. Crimes against property

Most computer crime laws focus on theft-type offenses and destruction of computers or computer system components. Questions arose about the adequacy of pre-computer crime laws to protect intangible assets [eg. P. v. Home Insurance, 121 P. 2d 491 (1978) holding information itself not the subject of theft - (a non-computer situation)]

Computer services are increasingly valued, and with the increase has been a growing awareness of the need to create specific protections for certain services. Wisconsin and Missouri have created additional penalties for damage to computers used by utilities, certain government operations, transportation, or other important uses. [Missouri Revised Statutes Sections 569.093-569.099, Computer Crime Law Reporter I-41-44; Wisconsin Statutes Annotated Section 943.70, Computer Crime Law Reporter I-77-

80.]

lc. Crimes against public morality

Though seriously (and I believe appropriately) undercut by a growing appreciation of the right to privacy, the criminal law continues to include attempts to impose moral values on society, often even in the absence of substantial harm to those committing the proscribed acts or to society at large. It is in this area that we find laws against certain intoxicants, certain sexual practices, and gambling.

Genesis magazine recently offered its readers a guide to "X-Rated Computers," explaining "You can use your computer as an information source or as a direct line to some really kinky folks. If Joseph Weizenbaum thought his little brainchild Eliza obscene when used to get people's heads straight, what would he think of a fifth generation "Eliza Domuch," a program designed to engage its users in sexual dialog?

Increasingly the concept of "addiction" is finding its way into conversations about computing, usually in the context of condemnation of "hackers." If the August 1984 Vanity Fair is right, and computers are the drugs of the future, will anti-computer addiction measures also be offered by the concerned Presidents' wives in the fifth generation? ["Wired to God" by Frank Rose, at 40.]

Lest we dismiss such concerns as beneath the dignity of the great and liberal city in which this conference is held contemplate the intersection of computer sex and computer addiction suggested by the movie Brainstorms. Though certainly beyond the current plans of the fifth generation, the possibilities for computer-aided and augmented masturbation are quite intriguing, and certain to arouse more than its proponents, if effective.

ld. Crimes against the maintainence of social order

Most subtle and least discussed of all types of crime that might involve greater risks in the fifth generation is corruption of the information on which modern society depends.

As litigation support becomes increasingly computerized, obstruction of justice by dishonest retrieval techniques

or secret filing systems will become a problem comparable to the keeping of second sets of books.

Public records are increasingly computerized. Their security will increasingly demand criminal protections.

Maryland is the first state known to the National Center which has specifically noted the need to protect public records from falsification through computer abuse [Laws of Maryland Section 45A, Computer Crime Law Reporter I-35]

B What acts shall fifth generation copmputer crime law deem criminal?

Since criminal law is coercive, and its stigma severe, its use is reserved for those whose behavior demonstrates culpability. The American Law Institute Model Penal Code limits guilt to those cases in which a person acts purposely, knowingly, recklessly or negligently.

As our references to "Hal," the 2001 computer demonstrate, the question of action becomes thorny when "artificial intelligence" enters the picture.

Three issues seem paramount:

1. Determination of the standard of care to be required-

Where the basis of a criminal charge is some form of failing to exercise adequate caution, recklessness or criminal negligence are required for criminal liability. Bassiouni notes "[m]ost statutes consider 'recklessness' as gross or serious disregard for the safety of others and require proof of conscious awareness of the condition created or of the potential consequences." [id. at 272] In Autonomous Technology Professor Winner argues that unpredictability is central to artificial intelligence. Where, we may ask with concern, does this leave criminal law? Is the use of an unpredictable instrumentality disregard for safety per se?

If we consider the law of vehicular homicide, an answer involving lower standards of care is suggested. Consider, for example, the doctrine in some states allowing failure to observe a traffic rule to constitute evidence of the driver's culpable negligence. Will failure to observe computer security regulations have the same effect?

2. Determining ultimate

responsibility-

Professor Gemignani suggests that computers may become the subject of regulation similar to that of nuclear energy: "If computers reach that point where they are so pervasive (and intrusive) in our lives that a massive failure of an important computer system could have consequences as disastrous as that of a failure of a nuclear reactor, perhaps a Price-Anderson Act for computers would not be unthinkable." [id. at 369 n. 105]

Expanding the concept, one may well ask whether the increased reliance on computers to perform the work previously done by professionals, as seems quite implicit in the growth of "expert systems," will not create just the sort of situation Gemignani suggests. In fact, he points out that we already have seen dangerous situations involving computer uses for air traffic control, nuclear plant monitoring, spaceship navigation, and interpretation of military data.

These increased uses of computers pose several political questions: Who will bear the risk of serious damage resulting from inadequate computer performance? Who will bear the burden of proving what occurred? What sort of standards of care will be imposed on users of computers? How will the user distribute the responsibilities to meet those standards of care among the personnel involved in programming, maintaining, operating, and securing those systems?

One possible answer is found in the predictions of Norval Morris, Dean of the University of Chicago Law School. "I predict that in our Third Century an Administrative Law of Crime will be devised....[for] our efforts to apply the criminal law to industrial, economic, health and welfare offenses." ["Criminal Law," in American Law: The Third Century at 95-99.]

It should be clear that the question of ultimate responsibility is a political one. Thus it is likely to be decided in the context of disaster putting the computer industry in a bad light. Will foresightful industry leaders prepare adequate safeguards to prevent such calamity from occurring? This is never an easy task, and is especially difficult in times of rapid and highly competitive economic expansion.

3. Assessment of causality-

A practical issue remains: proof.

Though we fear death through the agency of a robot, I suspect the much more difficult question is determining responsibility when death is the result of the performance of an undocumented program module. In a footnote discussing the Japanese crusher robot mentioned previously the author notes "there was some thought that it might have been caused by a defect in the computer program." [S. Lanoue, "Computer Software and Strict Products Liability," 20 San Diego Law Review, 439 (1983)] Thus far security functions like audit trails and good documentation have lagged far from the cutting edge of computer science. Is it reasonable to assume that the priorities will shift in the fifth generation? How often can you convince a salesperson to balance the checkbook rather than try to make another sale, or a scientist to delay an experiment in order to back up the results of the last one?

C. How shall fifth generation computer crimes be punished?

Punishment is central to the difference between civil and criminal law. Thus a major issue for the fifth generation computer crime law is the question of what to do with the criminal once we have convicted him or her. Unfortunately, little on the horizon indicates that society has moved past lex talionis. Though not so brutal as the Moslems who are still decapitating criminals, seizures of personal computers by FBI agents have a similar tone to them when done without process of law involving a judicial finding of guilt.

1. Theoretical problems

We have succeeded in refuting theories of correction, not supplanting them. Retribution is generally considered primitive and irrational, though it seems slightly on the rise. Rehabilitation is increasingly seen as an unfulfilled dream. (Given the abject corruption of prison environments, this should come as little surprise.) Deterrence of those inclined to commit crimes is still argued in every jurisdiction trying to decide whether to abolish --- or reinstitute -- the death penalty. The only reasonably clear observation is that incarceration incapacitates those who are so punished for the duration of their stay behind bars. (Unfortunately crimes within prison, including computer crimes, are not at all without precedent.)

We must, of course, declare certain behavior illegal even if none of our strategies seems particularly effective. One purpose of the Yugoslavian Criminal Code is "to exercise educational influence on other people [than the offender] in order to deter them from committing criminal offenses; [and] to influence development of social morals and social discipline among citizens." [Goldstein, Dershowitz, and Schwartz, Criminal Law at 724.]

trying to predict what needs to be protected, from whom, from what, and how.

Hart states a similar educational goal for American criminal law:

"To declare the obligation of every competent person to comply with (1) those standards of behavior which a responsible individual should know are imposed by the conditions of community life if the benefits of community living are to be realized, and (2) those further obligations of conduct, specially declared by the legislature, which the individual either in fact knows or has good reason to know he is supposed to comply with, and to prevent violations of these basic obligations of good citizenship by providing for public condemnation of the violations and appropriate treatment of the violators." [Hart, "The Aims of the Criminal Law," 23 Law and Contemporary Problems 401, 440 (1958) in Goldstein, Dershowitz and Schwartz, *id.*]

2. Practical resolutions

Undeterred by a lack of theory, much of the practice in computer crime punishment resembles the old football cheer, "hit 'em again harder, harder." Statutes calling for fines up to three times the property taken, enhancements of punishment for use of computers to commit other crimes, and special provisions for civil suits by crime victims have all been tried in recent computer crime laws.

As a former prosecutor I have seen the increased bureaucratization of criminal law. The process is typified by high volume case processing, high premiums on rapid turnover of cases, and most consistently, increased pleas bargaining. The paucity of cases of computer crime resulting in appeals underscores the universality of this trend.

Conclusion

The fifth generation will act as a magnifying glass, showing even more clearly the difficulties society faces