FIFTH GENERATION COMPUTER CRIME LAW

By Jay Bl omBecker
4053 JFK Library - Cali ornia State University
5151 State Universit Drive LA CA 900320

Director, National Cente 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 artic ial intelligence and expert systems research and applications. Wo will have to redefine crimes against the person/ property, public morality, and the public order. To do this will require considerable change in our standard.3 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 manifestions 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 politicans in power today.

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

Bruce Nussbaum, writing in The Wor1d After oil summarizes his fairly "straight forward 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 sustems 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 91.1

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.

Ia. 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 1-73; also see connect cut 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 1-10]

Section 18.2-152.5 of the Code of Virginia criminalizes "Computer invasion of privacy." [computer. crime law Reporter *1-73*]

Ib. 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 1-41-44; wisconsin Statutes Annotated Section 943.70, Computer Crime Law Reporter 1-77-

We must/ of course/ declare certain behavior illeqal 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 amonq citizens." [Goldstein, Dershowitz, and Schwartz, Criminal Law at 724.]

Hart states a similar educational goal for American criminal]aw:

"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 qood reason to know he is supposed to comply with, and to prevent violations of these basic obligations of good citizenship by providinq 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.]

?. 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 T have seen the increased bureaucratization of criminal Jaw. 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 trying to predict what needs to be protected/ from whom/ from what/ and how.