On the Global Dimension of Computer Legislation: A Third World Perspective

Article · May 1998

Source: CiteSeer

Adnan Yahya

Birzeit University

On the Global Dimension of Computer Legislation: A Third World Perspective

Adnan Yahya
Electrical Engineering Department,
Birzeit University, Birzeit, Palestine
Email:yahya@ee.birzeit.edu

Abstract

While information technology is playing an increasingly important role in all aspects of life in most countries, the rate of computer related crime is alarming. Steps are being taken in many countries to protect members of society against computer abuse. Matters are complicated by the multifaceted nature of information technology products and the rapid developments in the field. The level and nature of computer legislation vary from one country to another. The extensive cross-border exchange of information technology products makes coordination of legislation and law enforcement effort on the global level a prerequisite for success. However, computer legislation alone is not sufficient to combat computer crime. It needs to be supplemented by an effort to explain computer legislation and its positive effects on the quality of life, steps to educate the public on the ethics of computer use and with measures to reduce the appeal of such crimes. This paper addresses the issue of computer legislation and its global dimensions/implications with emphasis on issues pertaining to developing nations. It discusses the problems facing the application of traditional legislation to computer systems and the novel methods needed to account for the nonconventional nature of information technology products. We argue that consideration must be given to the international aspects of computer legislation in order for it to be efficient.

1 Introduction

The growing role of information technology in all aspects of human activity opens new prospects for development and creates certain problems for individuals and society. The widening use and abuse of computers and related systems mandate major steps on part of the legislature, professional societies, educational institutions and concerned individuals to encourage positive trends in the use of information technology, to regulate relations between the participants of the computerization process and to prohibit infringements on the rights of any member of society. These steps can take the shape of legislation on computer related activities, setting guidelines and ethical codes for data acquisition and manipulation, and educating the public on the risks and opportunities offered by information technology. Without a major effort to discipline information technology-related activities, considerable problems will be faced that may hamper economic development and negatively influence people's quality of life.

While the degree of computer introduction and its role and efficiency differ from one nation to another, the tendency towards more computerization is a worldwide phenomenon [1]. In addition, the large cross border trade in information technology products, developments in communications and networking activities and the resulting better access to computer systems from remote locations work to emphasize the global character of computer legislation. Without coordination on the international level, local legislation may prove inefficient in combating computer crime and encouraging positive developments in information technology. The alternative usually has the form of pressures by exporters of information technology products on consumer nations[5].

Computer related legislation and its implications carry special importance for the poorer developing nations of the world. These nations are dependent on the import of information technology products from richer industrial nations and very little is produced locally. This is usually a drain on the limited resources of foreign reserves and may lead to considerable underutilization of local skilled labor. The lack of proper computer legislation may have a fatal effect on the infant computer industry. It leads to flourishing black markets in computer products and negatively affects the computerization process.

2 Computer Crime

2.1 The Nature of Information Technology Products

Developments in information technology generated a wide spectrum of products to cater for the various needs of society. Although all these products are characterized by their reliance on computers, other properties differ substantially from one system to another. Even the term information technology product itself has a certain ambiguity due to the presence of computer components in many modern systems. Products differ, among other factors, in the importance and relative cost of their computer components, the generality of their use, methods of interaction with users, accessibility from remote locations and their internal structure and organization. This issue is complicated by the changing forms of man-machine interaction[5].

Computer products may exhibit behavior similar to that of more conventional systems but that behavior may be based on totally different design principles. For example, certain computer items have many similarities with traditional intellectual property. Computer programs are similar to written works but usually serve different functions. Computer graphics are similar to art work but the high repeatability and ease of copying and modification of programs and output limit these similarities. Furthermore, computers can be treated as regular machines in certain aspects but their programmability makes it possible for the user to radically alter their behavior. Access to computer networks and information therein can be treated as access to any other regular machines and files. However, the ease of access to computer systems independent of the distances involved and the nature of computer memory tend to blur these similarities.

As a result, dealing with information technology products under the rules of the pre computer era proved to be quite difficult[5, 21]. New issues come to light frequently as a result of rapid development in technology and its uses. Incorrect treatment of these issues in either direction can have major societal and/or economical implications[7, 12, 26].

2.2 Sources and Effects of Computer Crime

An important issue raised by the utilization of information technology products is the growing rate of computer related crime. We include here are all law violations dealing with computers and computer-stored information. Examples are software piracy, unauthorized access to systems and information, abuse of computer systems and information stored in them and many others[4, 13, 15, 19, 21, 23].

The problem is especially acute in developing countries where the rate of computer crime is very high. Software piracy is rampant and illegally acquired programs constitute the great majority, frequently more than 90% of the systems in use [29, 27]. Other computer crimes are taking place including unauthorized access to systems and data, introducing viruses to computer systems and violations of trade secrets and trade mark protection of computer products. It is frequently the case that computer products developed in industrial countries are beyond the reach of potential target groups in developing countries due to high prices. Additionally, differences in labor costs make the economic returns of computerized systems in financial or quality of service terms less attractive. Access to developments in information technology is limited due to economic, political or other factors[1, 9, 27].

The multifaceted nature of information technology products casts doubts on the applicability of existing legislation to computer related cases and raises a whole set of radically new issues for legislators to deal with. At present, legislation on computer related issues is still in its infancy and much is to be done in this regard[1].

2.2.1 Factors Encouraging Computer Crime

We believe that the following are important factors encouraging computer crime:

1. The high cost of computer resources which puts them beyond the reach of many people. This particularly applies to poorer nations where many of the popular programs cost more than the average annual per capita income for the country. This, combined with the lack of easy access to low-cost alternatives such as shareware and electronic bulletin boards make illegal acquisition the most realistic option to get access to certain computer products especially for private individuals [1, 27].

2. The relative ease of software piracy due to the ease of copying and the availability of products designed to facilitate access to systems and packages and the difficulty in tracing illegally acquired materials [21, 22].

3. The ambiguous nature of computer legislation and the doubts surrounding its applicability to specific actions. This is reflected in the outcomes of the major cases presented to the courts and the debate surrounding them[12, 17, 18, 21]. It is our observation that people are more at ease with pirating computer products than similar conventional items.

4. The weak level of literacy on ethical, legal, and societal issues in computing on part of computer professionals and the general public as well as the weak level of computer literacy and legal implications of computing of members of the judiciary and law enforcement personnel. Personal

[1] There were some instances when ancient, tribal law, was used to resolve program piracy disputes, in the expectation that extended litigation in the civil courts may not be able to resolve these cases promptly.

convictions about the need for computer software and information to be in the public domain and the imbalance in trade in these items often serve as excuses for unlawful actions[27].

5. The sophistication (real or perceived) needed to commit and hide computer crimes makes them look as an intellectual exercise and challenge rather than a common crime.

6. The snowball effect in computer crime. It is our observation that in areas where computer crime prevails, great pressure is exercised on individuals to avoid limiting themselves to legal means of acquisition and access. Elements like peer pressure and absence of social pressure to limit oneself to correct practices encourage computer crime.

2.2.2 Potential Effects of Computer Crime

Computer crime and failure to combat it will reflect negatively on the computer industry, the economic development as well as on the quality of life of the general public. Among these effects are the following:

1. The added cost of building open secure systems is passed to end-users resulting in higher cost of computer products and putting them out of reach of many potential users[6]. The cost of maintaining secure systems may prove prohibitive for individuals and organizations especially in poorer nations[14].

2. Crimes relating to software piracy and reverse engineering threaten the computer industry especially in developing nations. The availability of sophisticated, illegally acquired, imported products at nominal costs weakens competition and removes the incentive to develop indigenous, reasonably-priced computer products and makes it impossible for producers to recover the investment in research and development needed to build good systems with long-term support[2, 6].

3. The sense of insecurity and apprehension about the vulnerability of computer systems often leads to negative practices such as resorting to physical protection through cutting the systems from networks and severely limiting access to them[14, 25], reluctance to store valuable data in computer systems and excessive backup and validation effort. The more stringent mechanisms for systems, information and program protection are bound to complicate access to and use of these products and deter certain people from using them, more so in developing nations.

4. Pirated systems are not generally obtained with all the supporting material (documentation, updates, service). This prevents their optimal use. It is our observation that systems are frequently selected on the basis of availability free-of-cost rather than suitability for a particular application. The loss of revenue on part of suppliers may not enable them to offer good services even to legally acquired systems. All this will lead to an overall deterioration in the quality of the employed systems.

3 Computer Legislation

Even at the early stages of computing, system suppliers sought to apply existing legal protection mechanisms to their products. With the expansion of the role of information technology and the resulting increased threat of computer crime, the need arose for more elaborate legislation to deal with the many issues raised by the introduction of computers into the various aspects of life. Gradually, computer legislation and the legal implications of computing are becoming major topics of discussion at many forums.

3.1 Controversial Issues in Computer Legislation

The novelty and multifaceted nature of information technology products raise a whole set of issues that got to be addressed during the discussion on computer legislation. It is likely that answers will be country/culture dependent. Among these issues are the following:

1. The similarities between computer products and more conventional intellectual property and machinery. This includes similarities of computer programs, algorithms and computer stored information with more traditional types of intellectual property and similarities between computers, programs and computer controlled machinery with more traditional systems. Do the mechanisms for protecting intellectual property such as copyrights, patent laws, trade marks and trade secrets protection apply to computer products in their varied forms[12, 5, 17, 21]? Which parts of products can be covered by a particular protection mechanism and how far this protection can be granted without adversely affecting the industry[17, 10, 24, 28]? For how long protection can be extended in this rapidly changing technology? Which manifestations of the product are accorded a particular protection: the program, its output, the algorithm or the machine executing the program to generate the output if the program is machine dependent? Can protection be awarded to computerized versions of noncopyrightable material (old books, works of art...)? Is there a concept of partial protection in cases involving protectable and nonprotectable components (traditional works with translations,..)? How to protect the public from computer generated materials (films, illustrations,..)? Will a rating system be needed for this purpose especially with the expanding use of computers in education? Matters can get complicated with the use of multimedia concepts, the Internet and the World Wide Web[19, 21]. In cases when the crime is committed across national boundaries which jurisdiction should apply. The thorny issue of extraterritoriality may cause many problems.

2. The liability of manufacturers for any malfunctioning of their systems. This acquires special importance with the extensive use of information technology components in life-support systems, transportation, control of industrial processes and as basic tools in many business applications including the banking sector. Does this liability depend on such conditions as lack of criminal intent, the hiring of poorly qualified personnel, insufficient testing, the presence of inconsistent or erroneous data, failure to adhere to accepted standards, the use of inferior algorithms and the adoption of too ambitious design goals which are likely to lead to system failures[13]. This is compounded by the difficulty of detecting computer errors and the delayed nature of certain errors extending beyond the usual manufacturer's warranty period. A related

issue is the distribution of legal responsibility for failures of complex systems in which computer products are major parts. Who bears the responsibility for systems functioning well in stand-alone settings but generate problems when integrated into larger systems? How accurate and detailed manufacturers' information should be concerning the characteristics and possible uses of their products? Who is responsible for errors/delays resulting from malfunctioning communications systems in computer networks? Who is responsible for the effort to locate the sources of errors?

3. The admissibility of limited warranties and restrictions on use and distribution specified by manufacturers. Does the act of purchasing these products imply consent on part of the purchaser to comply with these terms? What about cases when these statements are written in a language or terms beyond the grasp of ordinary users? Is this in line with fair trade practices and the need to offer adequate protection to customers[10, 27]?

4. The distribution of blame in cases of proven computer crimes, such as those involving reverse engineering and performing software piracy, for hire. Should distributors of tools enabling unlawful access be held responsible for the damage resulting from the use of these tools in computer crime? Is the production and distribution of these tools a legitimate business[22]? Can restrictions be placed on the sale and acquisition of these systems to limit their uses to legitimate purposes and to prevent them falling in the hands of computer criminals? The legality of writing harmful computer programs and releasing them into computer systems and the stage at which such activities become illegal[7, 18, 21]. The issue of assigning liability to those involved in a computer crime is also troubling: who is more liable a person who places a program on for open access on the net or the one who copies it or both?

5. The degree of change a product must undergo to make it distinct from the original and to change the protection rights it enjoys. This is particularly important for the localization of information technology products to deal and interact with local languages. Will systems with different user interfaces be considered distinct from the originals[12, 27]? What about systems produced by the integration of many components including protected ones?

6. The balance between the privacy rights of individuals and the needs of the legal system including the balance between the interests of the prosecution and the accused of computer crimes. How much can be seized or subject to limitations on use to serve as evidence to prove/trace computer crimes? What about the cases involving multiple users of the same system and cases when it is difficult to establish ownership of resources? Will the mere possession of illegal material constitute a crime [20]? The legality of using computer methods to extract new pieces of information from available data. For example the use of deduction/statistical analysis techniques to construct profiles of certain individuals from legally available records.

3.2 The Global Aspects of Computer Legislation

Among the elements working to deepen the global nature of information technology are the export-import relationships between nations[11]. Most computer products originate in a small number of industrialized and newly industrialized nations and exported from there to the rest of the world.

Developing nations are almost always at the receiving end of this relationship due to the nonexistence or weakness of an indigenous computer industry[1, 3, 26]. Another element is the global networking activities, including the Internet/WWW, allowing fast access to major resources from any location in the world. Physical proximity to the site of the crime is not a needed for most computer crimes.

Legislation in one country cannot effectively deal with computer crime without major restrictions on the flow of information between nations. The problems are compounded by the rapid developments in information technology leading to novel systems and new methods for their compromise. Differences and inconsistencies in legislation between countries (and within individual countries) can create loopholes that reduce the effectiveness of local legislation and may even create safe havens for computer criminals[9]. Among the elements that got to be addressed in this regard are the following:

1. The heavy cross-border traffic in information technology products coupled with their extensive use in vital systems raise the issue of liability for damages between the suppliers of products and their users. This issue is more complex in the case of computer products than for traditional systems. Crimes are frequently committed across the borders of individual countries. The same act may constitute a crime in one location and be a perfectly legal act in another[9]. Safe havens for computer crime may be established that threaten computer-related activities worldwide. From such locations pirated software may be reexported to other locations and they can serve for tampering with systems through computer networks. Incriminating evidence may be hidden in foreign countries with the associated complications in proving the guilt of those accused of computer crimes.

2. In the absence of legal restraints, certain countries may be turned into dumping grounds for suspect information technology products. They may serve as testing grounds for experimental computerized life-support systems and destructive programs. The nonuniform distribution of expertise in the computer field may render certain nations defenseless against such practices.

3. Differences in the value systems and standards of living among cultures/countries may hamper protection against computer crime. A fine or a jail sentence that constitutes a deterrent in one country may prove out of proportion for another[12, 5]. The acceptability of certain laws my be problematic due to cultural differences. Information decency acts of different countries/cultures are bound to be different creating many problems for information exchange.

4. Differences in the admissibility of evidence and practices to prove guilt between countries. The debate on the admissibility of certain types of computer-related evidence and the amount of potential evidence that can be seized to prove computer-related crimes is under debate within specific countries. Differing outcomes of this debate in different countries will further complicate matters.

5. Differences in legislation, the overwhelming emphasis on legislation in industrialized countries, the ambiguity of the terminology used in these discussions outside the country concerned (e.g. the applicability of certain constitutional amendments of US constitution to computer-related issues), and the difficulties of understanding, say due to the language barrier, of the precautionary statements of copyright protection and limitations on use and liability may create major problems in proving intent in cases involving computer crimes[5, 10, 12].

6. Issues relating to restrictions on the free flow of information technology products between nations as a form of protectionist trade practices or to curtail information exchange between countries. This is complicated by the dominance of certain countries in the field, the difficulties in controlling the movement of information through national borders and the major linguistic and cultural component contained in many information technology products[1, 5, 12, 15, 26].

7. The role of regional and international organizations in the drafting and enforcement of laws dealing with computer crime. They can help in producing better legislation by sharing the accumulated experiences. This works to ensure comparable penalties for similar crimes and introduce a certain degree of uniformity of legislation especially in extensively interacting markets. Of value in this regard is the experience gained from international cooperation in similar fields such as copyright protection[23].

3.3 Measures Supporting Legislation

Despite its importance, legislation alone is not sufficient to combat computer crime. The need to offer fair hearing to the accused and the already alarming rate of computer crime will overwhelm the judicial system. Therefore, major steps must be taken towards the prevention of computer crime and the removal of its sources in the global context. These may include:

1. Setting ethical codes for dealing with information technology by professional associations and other interested institutions, preferably at the international level, and making these codes widely available to the public and maintaining campaigns to encourage adherence to these codes.

2. The introduction of material on legal and ethical considerations in the computer science curricula and computer literacy classes to nonspecialists and the introduction of computer awareness in the legal education of future members of the law enforcement system[26, 27]. Continuing education can be used to keep the interested individuals informed about developments in the field. Among the issues that must be covered is comparative computer legislation in various countries.

3. Accurate and responsible media coverage of computer crime and legislative and ethical issues to combat it in clear terms easily understandable to local the target population. Emphasis must be on the negative consequences of computer crime on the industry, economic development and the quality of life as compared to the positive effects of adherence to computer legislation on these elements.

4. A positive effort to create alternatives to guarantee access to information technology products to all nations and interested individuals. Special pricing policies such as those used in the case of text book production for poorer nations by major publishing companies with restrictions on reexport, the use of shareware concepts, easier access to global databases and networks and regional and international arrangements can be instrumental in advancing this goal[27].

4 Conclusion

The discussion in this paper reflected our belief that, short of resorting to isolationist practices, computer abuse can be effectively combated only in a global context. While computer crime may be directed against products and systems of a small group of countries, it is detrimental to the development of all nations including those where it is condoned. Therefore it is in the interest of everybody to participate in the effort to fight illegal practices and encourage positive developments. Since legislation alone is not adequate to deal with computer abuse, we believe that international cooperation must be extended to address some of the other problems characterizing the current state of affairs in information technology including the vast inequities between nations. However, international cooperation in these fields is not a substitute to the efforts taken in individual countries. The differences in the legal system, political structure, cultural setting, economic conditions and other factors require special treatment to account for the particular circumstances of each individual country.

References

[1] Abdallah, A. and Yahya, A.; Equity Problems in Information Technology: A Third Word Perspective; *Proceedings of the International Conference on Information Technology*; Tokyo, Japan, October 1990. Part 2, pp. 401-412.

[2] Arceneaux, J.; User-interface Copyrights Kill Competition; *Computer*; vol. 22, No 12; December 1989; pp.72-73.

[3] Bennet, J.M. and Kalman, R.E.(eds.); *Computers in Developing Nations.* North Holland Publishing Co. 1980.

[4] Cooper, L.; *Law and the Software Marketer*; Prentice Hall, 1988

[5] Cotters, S.; *International Intellectual Propoerty Law*; Wiley & Sons. 1995.

[6] Derwin, D.; Using Clean Room Design Procedures to Reduce the Legal Risk Involved in the Creation of Functionally Compatible Products; *Compcon 89*; 1989; pp. 379-385.

[7] Gemignani, M.; Viruses and Criminal Law; *CACM.* Vol. 32 No. 6. June 1989, pp. 669-671.

[8] B. Gerovac and R. Solomon; Protect Revenues, not Bits: Identify Your Intellectual Property; *Proceedings of IMA Intellectual Property Project* 1994.

[9] Ibramsha, M.; "Software Copy Protection Problem in the Muslim World: A Behavioral Solution; *Proceedings of the international Conference on Bilingual Computing*, Cambridge, U.K. September 1990.

[10] Kim, J. and Koen, C.; Software Piracy and Responsibilities of Educational Institutions; *Information and Management*, 18; pp. 189-194.

[11] Kaplan, G. (editor); EUROPOWER'92; *IEEE Spectrum.* Vol. 27 No. 6. June 1990; pp. 20-62.

[12] Lutfi, M.; *Legal Protection for Computer Programs*; Dar Thaqafa Publishers, Cairo, Egypt, 1987. (In Arabic).

[13] McFarland, M.; Ethics and the Safety of Computer Systems; *Computer*; vol. 24, No 2; February 1991; pp.72-75.

[14] McLeod, K.; Computer Insecurity; *Information Age*; Vol. 11, No 2; April 1988; pp.89-93.

[15] Nora, S. and Mink, A.; *The Computerization of Society*; MIT Press. 1980.

[16] F. Pomeranz; Technological Security; *Annals of AAPSS*, 498, July 1988. PP. 70-81.

[17] D. Remer and R. Dunaway; *Legal Care for Your Software.* Sybex, 1995. `http://www.island.com/LegalCare/`.

[18] Samuelson, P.; Can Hackers be Sued for Damages Caused by Computer Viruses; *CACM.* Vol. 32 No. 6. June 1989; pp. 661- 669.

[19] Samuelson, P.; Digital Media and the Law; *CACM.* Vol. 34 No. 10. October 1991; pp. 23-28.

[20] Samuelson, P.; The never-Ending Struggle for Balance *CACM.* Vol. 40 No. 5. May, 1997; pp. 17-21.

[21] Samuelson, P.; Legal Protection for Database Content; *CACM.* Vol. 39 No. 12. December,1991; pp. 17-23.

[22] Samuelson, P.; Regulation of Technologies to Protect Copyright Works; *CACM.* Vol. 39 No. 7. July, 1996; pp. 17-22.

[23] Sieber, U.; *The International Handbook of Computer Crime*; John Wiley & Sons, 1986

[24] Stern, R.; Micro Law- Software Patents; *IEEE Micro*; April 1990; pp. 8-11

[25] Wilkes, M. V.; Computer Security in the Business World; *CACM.* Vol. 33 No. 4. April 1990; pp. 399-401.

[26] Yahya, A.; Local Considerations in Computer Science Curricula Development; *20th Technical Symposium on Computer Science Education SIGCSE92*, St. Louis, Missouri, USA; March 1992. pp. 123-129.

[27] Yahya, A.; Software Protection: How Much is Enough; *Proceeding of the international Conference on Bilingual Computing*, Cambridge, U.K. September 1990. pp. 79-88.

[28] Yoches, E.R. and Levine, A. J.; Basic Principles of Copyright Protection for Computer Software; *CACM.* Vol. 32 No. 5. May 1989; pp. 541-545.

[29] Various Authors: `http://www.softwareprotection/com/`, `http://www.cs.ubc.ca/spider/day/CommEssay/section3_2.html`.