Technical Rips in the Seams of Intellectual Property Law: Sowing the Seeds of Information Assets Law

Anne W. Branscomb

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

Technical Rips in the Seams of Intellectual Property Law: Sowing the Seeds of Information Assets Law

Anne W. Branscomb
April 1992, P-92-2

Anne W. Branscomb is a legal scholar and president of the Raven Group. She is currently examining property interests in information as a research affiliate of the Harvard University Law School and the Program on Information Resources Policy.

This Report is the text of a presentation by Anne W. Branscomb that previously appeared in *The Annual Review*, a project of the Institute for Information Studies, a joint program of Northern Telecom Inc. and the Aspen Institute.

Printing 5 4 3 2 1

April 1992

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

ABRH Consulting, Inc.
Action for Children's Television
Advertising Mail Marketing Association
American Newspaper Publishers Association
American Telephone & Telegraph Co.
Ameritech Corporation
Apple Computer, Inc.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Bell Atlantic
Bell Canada
BellSouth Corporation
Boice Dunham Group Inc.
Bull, S.A. (France)
Centel Corporation
CMC Limited (India)
Commission of the European Communities
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Cox Enterprises, Inc.
Department of Communications (Canada)
Dialog Information Services, Inc.
Digital Equipment Corp.
DRI/McGraw Hill
European Parliament (Luxembourg)
France Telecom
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
Honeywell, Inc.
IBM Corp.
IQ, Inc.
Information Gatekeepers, Inc.
Information Industry Association
International Data Corp.
International Monetary Fund
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
I.T. Direction Ltd. (UK)
Japan Telecom Company
Kapor Family Foundation
Knowledge Industry Publications, Inc.
Korea Telecom
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
Martin Marietta
McCaw Cellular Communications, Inc.
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
Northeast Consulting Resources, Inc.
Northern Telecom
Nova Systems Inc.
NYNEX
Ing. C. Olivetti & Co., S.p.A. (Italy)
OTC Limited (Australia)
Pacific Telesis Group
Public Agenda Foundation
Puerto Rico Telephone Co.
Research Institute of Telecommunications and Economics (Japan)
RESEAU (Italy)
Revista Nacional de Telematica (Brazil)
Salomon Brothers
Scaife Family Charitable Trusts
SEAT S.P.A. (Italy)
Siemens Corp.
Southam Inc.
Southern New England Telecommunications Corp.
Sprint Corp.
State of California Public Utilities Commission
TEKNIBANK S.p.A. (Italy)
The College Board
Times Mirror Co.
Tribune Company
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of State
  - Office of Communications
- Federal Communications Commission
- General Services Administration
- National Aeronautics and Space Administration
- National Security Agency
- U.S. General Accounting Office
- United States Postal Rate Commission

US West

ACKNOWLEDGMENTS

The author gratefully acknowledges the very kind help of the following people who reviewed and commented critically on the draft of this report. Without their consideration, suggestions, and encouragement, this study could not have been completed.

Robert P. Bigelow
JoAnne G. Bloom
Jack E. Brown
Stephen Y. Chow
Steen B. Frandsen
Roy Heath
Michael A. Jacobs
Brian Kahin
Michael S. Keplinger
Peter B. Maggs
Vanessa Marsland
Nicholas P. Miller
Vincent Mosco
Mark S. Nadel
Arthur Oppenheimer
John Rothman
Pamela Samuelson
Peter Sandler
Victor Siber
Oliver R. Smoot
Joan E. Trusty
W. Russell Wayman
Stanley P. Witkow

These reviewers and the Program's affiliates, however, are not responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

EXECUTIVE SUMMARY

Intellectual property is an arcane subject of interest primarily to lawyers and their clients in the business of marketing copyrightable literary and artistic works or manufacturing patentable products and processes. Indeed, the word "property" is considered by many purists to be a misnomer, because they find it difficult to apply proprietary concepts to information resources that remain available to the original owner while disseminated to many others users.

With the growing privatization of the information marketplace and the proliferation of information products, economists are grappling with the value of "information" or intellectual productivity as a commodity. Lawyers are reaching to apply traditional copyright, patent, trade mark, and trade secret laws to newer outpourings of information technology which often do not comfortably fit within the established legal precepts.

With large databases collecting and collating facts and figures, which are not the subject of copyright protection, an increasing concern has arisen about the legal rights of individuals as well as institutions to prohibit access to such information pertaining to their individual and special interests. This body of law has come to be recognized as privacy protection.

A new field of law which may be called the law of "information assets" is developing that encompasses both the products of human creativity (generally protected as "intellectual property") and the known or knowable attributes surrounding persons, corporations, or other legal entities that can be controlled (generally protected as "privacy" or "confidentiality").

This paper explores selected areas in this murky legal domain where challenging questions are being asked and rational (and sometimes irrational or transitional) solutions are being crafted. These include:

- Attempts to cope with unauthorized intruders and abuses of information on computer networks and databases
- Efforts to achieve compatibility through modification of the "fair use" and "reverse engineering" concepts
- Searches for integrity of information in the environment of computer graphics, colorization, and audio editing
- Changes in the boundaries between the public and private domain
- Exploration of new forums for the resolution of disputes about the use and misuse of information
- Bypass of traditional institutions through initiatives in the GATT and European Community

- New threats to privacy from automated telephone number identification and direct mail merchandizing

The legal regimes under which information assets are protected appear to be bursting at the seams. To many observers, current efforts seem to be hammering square pegs into round holes. Rather than the fit of the perfect glove, current practices seem more like cutting off the tips of sailors' gloves to accommodate the apparel to the wiles of the weather, while permitting dexterity in handling of the rigging. The question is, how many holes can you cut before you have a completely different legal fabric or none at all.

The universe of activities affecting legal rights in information assets is vast. Pioneering efforts are going forward in many arenas, but participants rarely connect beyond the boundaries of each limited domain. Both creators and users of information are seeking new avenues for protecting and exploiting information assets. This paper identifies a number of issues and institutional environments in which new modes of operation are being explored and new accommodations being reached.

CONTENTS

PREFACE

CAVEATS, COMMENTS, AND UPDATES

This paper was a snapshot in time, taken at mid-year 1990, intended to examine a number of developments in the treatment of the law of information content (or information assets). The predominant, but not the sole, legal regime applicable to the control of information assets is intellectual property law, itself a mixture of legal regimes, including copyright and patents, each with its own separate and often independent bar. Only recently, with the advent of litigation over the applicability of these two regimes to computer software, has the bar attempted to wrestle with both regimes simultaneously.

The concept of privacy, which developed separately and apart from traditional concepts of intellectual property law, also affects information content, especially as it is archived, manipulated, and transmitted over telecommunications lines. Several reviewers questioned whether new concerns – agitation over caller ID, automated number identification, and the marketing of transaction generated or consumer-oriented personal data – should be included in a discussion of "Technological Rips in the Seams of Intellectual Property Law." Some reviewers saw no relationship between privacy and intellectual property. My rationale is that privacy laws afford a legal right to control the access to and use of information akin to the right to withhold publication under copyright statutes. Others were offended by the suggestion that "rips" existed in the seams of legal systems deemed infinitely malleable to suit any situation that the new information technologies might throw at them. Thus, if some readers seem needlessly myopic and others overly confident, my hope is to expand the horizons of the former and test the bravado of the latter.

The laws of libel, privacy, copyright, and patents, when viewed from the perspective of an outsider attempting an overview of many different areas, all seem to have aspects that pertain to the ownership and control of information.

My title may have been ill chosen, but lawyers, and the author is no exception, traditionally build on what already exists, and I meant the title as a platform for an examination of the many developments in the application of new information technologies that emphasize those two existing legal regimes. Several areas of recent ferment portend a need to reexamine ways in which information content is treated in technologically advanced computerized information systems.

If another study of this type is attempted, it might more wisely be called an attempt to define the dividing lines separating public, proprietary, and private information domains, and because these lines blur and overlap, the task is ambitious, demanding the skills of many activists and critics. This paper is an effort to open doors to a better understanding of how the laws of information societies treat information content. The number of reviewers who offered commentary would seem to confirm that others also view the current state of the law as quite turbulent and challenging.

The purpose of this preface is to look at major developments since the paper was first published as a chapter in the Aspen Institute's Annual Review of Communications 1990. As many reviewers noted, current events fast become ancient history in the saga of the legal treatment of information content, and, indeed, between the paper's first publication and its circulation as a draft by the Program on Information Resources Policy (1991), a number of actions had overtaken concerns expressed in it.

COMMENTS ON INDIVIDUAL CHAPTERS

Chapter One: Applying Criminal and Civil Laws to Miscreant Behavior

The United Kingdom enacted its "proposed law" on computer hackers, which on July 31, 1990, became a statute titled "The Computer Misuse Act of 1990." The first conviction was achieved on March 20, 1991, when David Pearlstone was found guilty of unauthorized access with intent to

commit or facilitate the commission of another offense, that of "false accounting." A spokesman for Scotland Yard indicated the problem area which seemed likely to inhibit further convictions would be showing that the perpetrator knew the access was unauthorized.

In the United States the conviction of Robert T. Morris, Jr.,[1] by the Northern District of New York was upheld by the Second Circuit[2] and the writ for certiorari denied by the Supreme Court, laying to rest speculation that the judge's ruling concerning the necessity only to show the intent to insert the virus into the Internet and not an actual showing of malice was sufficient for conviction.[3]

Nonetheless, the Senate of the 101st Congress passed an amendment to clarify that "negligent disregard" of the consequences would be sufficient to find a culprit guilty of a crime rather than specific mal intent to cause the consequences resulting from the culpable act. The legislation S.1311 (The Computer Abuse Amendments Bill) was reintroduced into the 102nd Congress and incorporated into S.1241, the Violent Crime Control Bill of 1991. Legislation was introduced by Senator Orrin Hatch (Utah) to impose criminal penalties for violations of software copyright (S. 893).

The U.S. Department of Justice is showing greater diligence than in the past in tracking down and prosecuting miscreants who used computers and networks.[4] When Craig Neidorf's equipment was confiscated because used to disseminate allegedly proprietary information concerning BellSouth's 900 system, widespread concern about abuse of civil liberties led to the establishment of an Electronic Frontier Foundation (EFF). The EFF is devoted to the maintenance of first amendment values along the new frontiers of electronic space.

Steen B. Frandsen, Senior Managing Partner of Frandsen van Beek, Certified Management Consultants (Toronto), offered a reminder that the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Havana, Cuba, 27 August to 7 September 1990) issued a call for member nations "to intensify their efforts to more

effectively combat computer abuses that deserve the application of criminal sanctions at the national level" and especially to consider "becoming parties to treaties on extradition and mutual assistance in criminal matters which can accommodate the particular problems pertaining to computer-related crimes."[5]

Another significant effort to encourage harmonization of criminal sanctions against computer abuses is taking place within the Organization for Economic Cooperation and Development (OECD), where Justice Michael Kirby of Australia is leading a study group to make recommendations to OECD's member nations.

Whether computer files can be considered "stolen property" for the purposes of a criminal indictment has come up in two recent cases with directly contradictory results. In U.S. v. Riggs[6] the Northern District of Illinois held that a stolen text file in machine readable form was a tangible "good" within the meaning of the statutes prohibiting interstate transportation of stolen goods. The Tenth Circuit Court of Appeals, while acknowledging its disagreement with the decision in U.S. v. Riggs, determined in U.S. v. Brown that source code could not be so considered.[7] The ramifications of a holding that computer files may be "tangible property" became apparent when a Florida court held that the sale of electronically displayed financial information could not be subject to the Florida sales and use tax, because such transactions did not involve the sale of tangible personal property.[8]

Chapter Three: Ownership of Federally Generated Information Resources

Concern about a need for authority to transfer copyright interests in federally generated software continues. In 1990, the General Services Administration (GSA) issued a report on constraints on commercialization of federal software by some federal agencies to facilitate transfer of information technology to the private sector.[9] Legislation was introduced to permit government agencies developing software in consortia with private companies or educational institutions to transfer

copyright interests to the party assuming responsibility for use in the private sector.[10] Hearings on S. 1581, the Technology Transfer Improvements Act of 1991, were held on September 13, 1991; the Copyright Office supported this limited effort to motivate federal employees with the prospect of financial benefit from exploitation of their software by private sector entities.

Some reviewers expressed concern that the paper overemphasized the public interest in privatizing government generated information assets represented by this policy directive. They urged that much public domain software is used as a platform by independent software developers to innovate their own products. The trend toward privatization of information assets generated by government funds might inhibit what many scholars consider the healthy circulation of such software among small, independent entrepreneurs who design and produce innovative products.

Counsel for Ashton-Tate (recently acquired by Borland) expressed doubt that the lack of copyright protection inhibited the transfer of technology to the private sector, pointing out that the popular dBase product was inspired by a public domain product. This experience is not unique. Other popular proprietary products have enjoyed commercial success while claiming copyright protection for their value added to a public domain platform. Peter B. Maggs, Professor of Law at the University of Illinois, doubted that software placed in the public domain languishes unused, pointing out the success, for example, of West Publishing in commercializing the distribution of public domain statutes and case law.

Chapter Four: Trips in the Uruguay Round

The December 1990 meeting of the Uruguay Round of the General Agreement on Tariffs and Trade (GATT) was disappointing in its failure to reach agreement on many subjects, especially its inability to reach consensus on the initiatives to incorporate a regime for handling intellectual property rights (particularly trade secrets) into the GATT.

The U.S. Special Trade Representative (USSTR), however, has not given up hope of ultimately reaching an accommodation within the GATT framework. Several reviewers commented on the unsatisfactory state of international organizations in dealing effectively with such issues and hoped that more innovative ways of resolving such disputes could be found.

The high priority for the U.S. of the GATT negotiations was emphasized in Senate hearings on May 15, 1991, before the House Judiciary Committee's Subcommittee on Intellectual Property and Judicial Administration. The unresolved issues focused on by the hearings included: the extent of protection for computer programs, the applicability of rental rights, use of local trademarks with foreign trademarks, standards of protection for industrial designs, exceptions to patentability and the term of the patents, the scope of protection for semiconductors, and whether to include trade secret protection. An area of disagreement between the computer industries of the U.S. and Japan is the nature and amount of "reverse engineering" or decompilation of code.[11]

Chapter Five: Private Alternatives to Judicial Procedures: The IBM-Fujitsu Arbitration

There is little evidence that arbitration has become the avenue of choice for international disputes over intellectual property rights, which may give way to more agitation for regional, sectoral, or international arrangements for the resolution of disagreements.

Michael Jacobs, counsel for Fujitsu, pointing to the published opinions in the IBM-Fujitsu suit, commented that the paper gave short shrift to the arbitration between IBM and Fujitsu, used here as an example of potentially complex transborder litigation that the parties could handle with more control than the judicial alternative. The arbitration was conducted to clarify rights under a prior settlement agreement concerning the use by Fujitsu of "IBM compatible mainframe operating system software products" which allowed Fujitsu a reasonable

opportunity to develop independently and maintain IBM-compatible operating system software by permitting Fujitsu access to a "secured facility" of IBM for a period of five to ten years. Fujitsu paid a lump sum to IBM for the resolution of past disputes and will pay for future access assured in the arbitration decree.

Essentially, counsel for Fujitsu denied that Fujitsu claimed that the operating system software under dispute should be in the public domain. According to Fujitsu, the versions used either were uncopyrighted or did not constitute protectable expression, because certain functional characteristics had in effect become industry standards; Fujitsu claimed that it must use them in order to compete with IBM's mainframe operating systems.

Counsel for Fujitsu objected to the statement that Fujitsu would be excluded from access to a secured facility of IBM. According to the then intellectual property laws, Fujitsu would have as much access to intellectual property developed by IBM as any other competitor. What the paper was intended to convey was that Fujitsu would then be excluded to the same extent as other competitors and enjoy no special privileges such as had heretofore attached to the arbitration decree.

The complexity of such disputes may be one of the reasons that arbitration as the forum of choice for transnational litigants has not proliferated. Professor Maggs chided the author for suggesting that arbitration was inherently second-best to litigation. If so, this was a misunderstanding, because I meant just the opposite, to suggest that many consider arbitration superior to litigation for the reasons given by Professor Maggs:

> Many, many business executives and lawyers think of arbitration as inherently better than adjudication. They see the great need as being in development not of legal institutions that would handle disputes in court, but of legal institutions that would encourage and support arbitration and so enable them of stay out of court.

Nonetheless, rather than an increase in the use of arbitration, more consensual efforts such as those initiated within the EC and the GATT are occurring, in a trend, as Arthur Oppenheimer, of American Express Europe Limited (England), commented, toward forums "where legal definitions are replaced by panels of experts whose goal is arbitration and consensus in place of legal arguments or case law." Pamela Samuelson, Professor of Law at the University of Pittsburgh, has noted that one of the major disadvantages of arbitration is that it provides no legal precedent that is binding on subsequent attempts to resolve disputes.

Chapter Six: The Video Marketplace

In 1990 the U.S. Congress passed an amendment to the copyright laws to prohibit the rental of computer software without the consent of the owner of the copyright (S.198).[12] The European Community (EC) included a similar prohibition within the council directive on the legal protection of computer programs.[13]

Several reviewers commented that the discussion of colorization of old black and white movies was inaccurate or confusing or both. I pointed out that any person having access to the black and white version, now in the public domain, could render a colorized version (or make any other use of it) but not copy any other colorized copyrighted version. This is the correct legal situation, and my statement that colorization "can extend" the life of the copyright beyond the original time period was an inept attempt to say that as a practical matter colorization of black and white video products tends to extend a de facto monopoly over the use of material for which the copyright protection has expired.

Several reviewers suggested that more of the discussion should have been devoted to multi-media products and the legal implications incumbent on their development, certainly, this area deserves adequate analysis and should be developed in future work. As the use of the

personal computer becomes more ubiquitous, access to networking more prevalent, and the marriage with laser discs more normal, the questions of who can use which digitized data for what purposes will become increasingly critical.[14]

Chapter Seven: Computer Software Protection in the European Community

At the time this paper was written (1990), the debate and disagreements about protection of software were in full swing. The Draft Directive of the Council of the European Communities on the Protection of Computer Software, enacted on May 14, 1991, recognizes copyright as the appropriate legal regime under which computer software should be protected by member states "as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works."[15] Ideas and principles are excluded from protection, including those underlying interfaces. Furthermore, the right to use back-up copies includes a right "to observe, study, or test the function of the program in order to determine ideas and principles which underlie any element of the program," so long as such observation is achieved through normal use of the product to which the person so observing is entitled.[16] Rental rights, as noted above, "shall be subject to authorization by the rightholder,"[17] but such rights do not seem as circumscribed as those conferred by the U.S. Congress.

The controversial area of "reverse engineering" has been modified to confer only a very restricted right of "decompilation" when "indispensable to obtain the information necessary to achieve the interoperability of an independently created computer with other programs."[18] The directives specifically warn against the use of such decompilation right for the "development, production, or marketing of a computer program substantially similar in its expression, or any other act which infringes copyright."[19]

Because the directive does not, of course, become effective statutory law without enabling legislation from the member states, the challenge

for European legislative bodies will be to come up with complying statutes before the target date of January 1, 1993. This will require some sorting out of terms of protection, levels of originality required for coverage of copyright protection, and, especially, concise and comprehensible definitions of what "interoperability" really means in a legal sense.

Chapter Eight: Automated Number Identification

Some reviewers, while admitting that automated number identification (popularly called "Caller ID") was an interesting controversy, found it out of context in a discussion of property rights in information. Although a telephone number, standing alone, may seem an unlikely legal entity, the right to control who may assign and use or transfer the right to use the number is a matter of considerable value and concern. Within a very few years, given the present system of ten digits, the numbers available to assign users will be exhausted. With personal telephone number assignments well within the vision of the near future, questions touching on their distribution and whether they can be used for other purposes of identification and, indeed, become a commodity on the open marketplace may soon arise. At present, the telephone number itself is becoming an almost universal identifier as many direct mail and telephone merchandisers seek to obtain and use them for their computer files as identifiers of customers.

Moreover, the recent determination by the Supreme Court in Feist v. Rural Telephone,[20] that the telephone number is incapable of coverage by the copyright laws, will lead to agitation for legislation or litigation to sort out what proprietary rights can be asserted to control the allocation and use of numbers, because they are a marketable and valuable information asset.[21] According to the Feist decision, a telephone directory, which was shown to be drawn without authorization from the petitioners' telephone list, was an uncopyrightable work. According to Justice O'Connor, copyrightable works must have a modicum

of "original expression" in order to qualify for suits for infringement, which a telephone directory of raw numbers does not.[22]

This landmark decision has implications more far-reaching than coverage of mere telephone numbers, because it will affect the constitutional limitations of the copyright act to cover other factual data that form the foundation of most computerized databases. Litigation or legislation or both will, in due course, sort out to what extent a competitor may copy or re-use factual data within a competing product, so long as they do not copy any protected "original expression." What Justice O'Connor has accomplished is creation of a roadblock to expansion of copyright law to cover facts assembled in databases by tracing the opinion to constitutional roots.[23] Furthermore, the Court explicitly rejected the line of cases developing a "sweat of the brow" theory to justify protection of such compilations, to wit, "copyright protects originality not effort."[24]

The agitation over the use of telephone numbers grows more complex with each passing year, as technological advances make both automatic solicitations easier and technological blocking devices more practical. Those concerned about unsolicited calls should refer to a comprehensive study of these issues by Mark S. Nadel.[25]

Clearly, how telephone numbers are issued, used, protected, and marketed will increasingly come to the fore in public debate as users become increasingly agitated about their deployment. Companies will confront the costs and inconveniences of providing technological "fixes" for consumer option in the disclosure of telephone numbers as well as access to them for a variety of legitimate reasons.

Chapter Nine: Marketing of Consumer-oriented Personal Data

Comments from reviewers confirmed that the treatment of personal data within highly sophisticated computerized communications systems is a

matter of growing concern. Joan Trusty, Associate General Counsel, Electronic Data Systems Corporation, commented:

> ...who owns personal information? If the information on what car you drive, your buying preference, your income, and your level of credit card usage is seen as personal information which is owned by you, then arguably compensation should attach for the sale or commercial use of your property. If the information is not seen as my property, nonetheless, does some level of privacy protection attach to it? Finally, if the information is seen as "not property," and "not private," have we now created two levels of personal information (regardless of how an individual feels about that information) – protected personal information and unprotected personal information? Thus, private information could be that which one discloses on one's tax return, but the amount filled in as "annual income" on a credit card application is not private. Also, whether information is private or not can depend on circumstances – while I might not mind whether anyone knew that I preferred Diet Pepsi to Diet Coke, the national spokesperson for Diet Coke might not want it be known that he/she really buys Diet Pepsi at his/her local supermarket.

That a user revolt may be in the offing to exert more personal control over the collection and distribution of personal information was indicated by the uproar over the announcement of a new laser disk "Lotus Marketplace" product offered in early 1991. Lotus Development Corporation, with Equifax Marketing Decision Systems, put together an optical disk that contained information on more than 80 million households and some 120 million individuals, to provide small entrepreneurs access to marketing information that Equifax and other collectors and collators of market-oriented data routinely supplied to large companies.

Despite protestations that efforts had been made to protect the accuracy of the data and provide opportunities for individuals to have their names removed from the database, opposition developed so rapidly (much through Internet and other electronic networks) that 30,000 letters of protest prompted Lotus and Equifax to withdraw the product.[26]

Efforts are also going forward within the EC to promulgate directives with respect to protection of personal data and privacy in public

digital telecommunications networks.[27] European nations have a long history of concern with manipulation of personal data in computerized databases, and many of them have established bureaucracies experienced in dealing with personal data. The U.S., although without the assistance of Data Commissioners or a complex bureaucracy, has nonetheless enacted a spider web of laws governing the use of personal data which may well equal the developments in Europe, except that the U.S. laws are primarily concerned with prohibiting the excesses by federal agencies in the collection and use of personal data rather than with imposing substantial rules on private entities.[28]

Conclusions Concerning Comments

More than twenty reviewers voluntarily submitted comments on this paper, in the gamut from outrage to admiration. Many shared their own concerns and apprehensions, as well as thoughtful proposals for future consideration. Clearly there is no consensus on an optimum legal approach to the advent of technologically sophisticated and complex information assets in the burgeoning "information marketplace."

Many of the reviewers are comfortable with the piecemeal approach through diverse litigation and modest modifications of legislation in the United States, while others long for a more coherent and comprehensive overview. Some welcome the major initiatives within the EC, while others view them with alarm.

Some were enthusiastic about the attempt to collect and organize currently applicable principles governing deployment of information assets, while others look on such efforts as destined for failure until greater experience has been gained through long exposure to the changing landscape.

What became apparent is that satisfaction with the status quo is not so widespread as some hope. Neither is the erosion of present law irreversible. Regardless of these diverse and nonconvergent views,

initiatives are going forward in a number of forums – state, national, international, and transnational – all dealing with some aspects, often very different ones, of information ownership and control.

One of the more protracted debates, which the paper does not touch on at all,[29] is the litigation and agitation for legislation dealing with computer software. These concerns involve a number of issues. One is concern that the increasing number of patents granted for software inventions will stultify a rapidly growing software industry. Another, of great concern to network users and service providers,[30] is whether the trend of the courts to offer greater protection to user interfaces impedes interoperability. The groundwork is being laid for reconsideration of some of these issues; the Patent Office has set up a new commission to take a major look at the patenting process, including the treatment of computer software, and the Office of Technology Assessment has undertaken a new study of computer software at the behest of the House Committee on the Judiciary.

Whether the attempt to forge a unified approach to the analysis of the legal infrastructure for the deployment of information assets is useful remains questionable. As Peter Sandler, Head of Sector of the Commission of the European Communities (Brussels), commented:

> [I]n an area raising so many disparate problems solutions are bound to be on a piecemeal basis. In some areas answers will be found in adapting existing IPR protection, whilst in other cases new rights will have to be created.... This is all the more likely as solutions will represent a compromise between competing national interests and traditions, and perhaps the best we can hope for any solution is that "nobody will be happy."

Stakeholders vary in their interests and will pick and choose the arenas where it is expedient for them to participate in ongoing debates. Globalization is changing the nature of the landscape in which to battle, and national laws are not well conceived to operate internationally or multilaterally. Difficulties abound in attempts to apply laws outside the territorial jurisdiction. Today's competitors spill over these tightly drawn lines and interact competitively,

cooperatively, and occasionally consensually. Nothing indicates that the establishment within the information world of boundary lines between what is a public or private domain will be any easier than in the world of real property or, indeed, of the open seas. This paper is but one small effort at an overview of the legal landscape in which information assets put down their roots.

CHAPTER ONE

INTRODUCTION

Intellectual property historically has been a rather arcane subject, of interest primarily to lawyers who specialized in copyright, patent, trade secret or trademark practice and to their clients in the manufacturing, publishing, or motion picture industries. Indeed, the use of the word "property" has bothered many purists who argue that an "information product" cannot be the subject of alienation or possession in the same way that a piece of real estate can be unique to the particular owner or owners.

Attempts to prosecute information pirates under the usual laws of theft and embezzlement ran afoul of the requirement that the alienation be subject to an intent to "deprive the owner of the use thereof." More fundamental, information economists have attempted to grapple with the value of "information" or intellectual productivity as a commodity. Most find it difficult to cope with a resource that remains available to the original owner while yet disseminated to many other users.

It is from this murky domain that intellectual property laws have emerged to cope with licensing of manufacturing processes, the marketing of artistic and literary works, and more recently with the outpouring of computer software and databases which have accompanied the arrival of the much heralded "information age." With large databases collecting and collating facts and figures, both aggregated and personally identifiable, an increasing concern has arisen about the legal rights of individuals as well as institutions to prohibit access to such information pertaining to their individual and special interests. This body of law has come to be recognized as privacy protection.

However, both intellectual property and privacy are aspects of a broader and developing field of law which encompasses both the products of human creativity (generally protected as "intellectual property") and the known or knowable attributes surrounding persons, corporations, or other legal entities which can be controlled (generally protected as

"privacy" or "confidentiality"). Together, they might be called "information assets."

Along with the advent of new modes of information processing has come a proliferation of devices through which such information assets can be easily copied, reprocessed, manipulated, mangled, or destroyed. Even more important the diversity of nodes to the global telecommunications grid gives access to a wider range of imaginative opportunists who invent new and different ways of exploiting the brain children of their more innovative and/or productive colleagues and competitors. At the same time, the increasing numbers of nodes provide access to information assets across national boundaries undreamed of by the European mariners who explored the seven seas looking for new and commercially valuable products to enrich their coffers and enhance their reputations. Therefore, the law, the technology, and the economics of information seem to be converging upon a propitious historical moment for reorienting their traditional paradigms to accommodate a rapidly changing global environment.

Moreover, the traditional balancing act between public and private interests has become more and more difficult to achieve. The interests of producers of information assets and the users thereof often clash. The interests of sources of information assets and those who wish to exploit them do not necessarily coincide.

These conflicts of interest render a review of recent developments in intellectual property and privacy law an extremely difficult task. The landscape is so vast that only a fool would undertake to execute the task in a comprehensive and exhaustive manner. Consequently, the current paper will address selected areas in which challenging questions are being asked and where rational, if sometimes only transitional, solutions are being crafted.

These include a look at some of the following developments:

- Grappling with new intrusions on networks and databases by computer viruses, worms, Trojan horses, and logic bombs;

- Striving toward compatibility in the "look and feel" cases governing computer software and the litigation over use of proprietary pagination by LEXIS and Westlaw;

- Modifying existing laws which are culturally and nationally bound to accommodate to the global information marketplace;

- Searching for integrity in the controversy over colorization of old movies, transformation of recognized work products through the use of computer graphics, the aping of distinctive voice characteristics and the replication of proprietary images or choreography;

- Exploring new forums for resolution of disputes such as the international arbitration agreement between Fujitsu and IBM;

- Bypassing of existing international institutions through initiatives in the GATT to incorporate an international legal regime for intellectual property through the use of the trade agreements system;

- Accommodating existing regulatory requirements to the changing needs of new technologies;

- Combatting new threats to privacy from automated telephone number identification and direct mail merchandising.

Legal Luddites worship at the shrine of copyright law and laud its infinite capability to weave a web around each new technology that appears on the horizon. Yet the complexity which surrounds the discussions of legal applicability, as well as the diversity of forums in which stresses are being evidenced, belies their confidence.

The legal regimes under which intellectual property is currently protected seem to be bursting at the seams. To many observers current efforts appear to be hammering square pegs into round holes. Rather than the fit of the perfect glove, current practices seem to be more like cutting the tips off the gloves of sailors to accommodate the apparel to the wiles of the weather, while permitting dexterity in the handling of rigging. The question is how many holes you can cut before you have a completely different legal fabric or no fabric at all.

The universe of activities affecting legal rights in information is vast. Ferment can be detected in many environments. The inescapable

conclusion is that better protection of information assets is a primary goal for developed economies whereas greater access to information assets is a major goal of developing economies. These two perspectives are not necessarily inconsistent, but consensus on the appropriate line between the two views is not easy to locate.

Pioneering efforts are going forward in many arenas. Rethinking of time-honored concepts is taking place with such concepts as "fair use," "reverse engineering," "first sale," "moral rights," and "compulsory licensing."[31] What follows is a stroll through this maze of often conflicting and confounding developments.

CHAPTER TWO

APPLYING THE CRIMINAL AND CIVIL LAWS TO MISCREANT BEHAVIOR

"Property" is a concept that is alien to a sharing or socialist society which looks upon all assets (especially intellectual assets) as "belonging" to the body politic, or the manifestation of the generosity of a benevolent god, or devoted to achieving the "common good." Yet there never has been a time in history when covetousness was not apparent, theft used as strategy for improving one's economic well-being, hoarding practiced by many to increase their security, and secrecy used as a fallback for protecting assets.

Part of the trouble with current unrest with respect to so-called computer crime is that part of it is just that – what in other environments would be a criminal act except that the act is aided or abetted with the use of a computer. Another part is more akin to fraternal jokes played on one or another of one's friends or enemies to get even after a presumed slight. Where to draw the line between the prohibited and the permissible is never easy but has been made far more complex with the advent of an entire new array of gadgets and machines with which the usual "takings," "disruptions," and "disturbances" can be accomplished.

Many of today's young computer whiz kids were brought up in an ethical environment which challenged them to break into anybody's computer who tried to prohibit entry. For some this was a game. For others, it was a challenge to develop skills. For a few it was a philosophical crusade to achieve that openness and spirit of cooperation which achieves greatness through building upon the "shoulders of giants."[32] So long as the devastation was as small as that accomplished by the "cookie monster," which devoured a student's working data on his or her PC, such pranks were not a matter of national import.

As the number of personal computers used worldwide accelerates into the tens of millions and the number of computer networks increases at a

comparable rate, the concerns of computer users that their memories and connections be secure and reliable becomes paramount. What is contained in those memories and whirling through the electronic ROMS and RAMS, whether it be "property" or not, represents valuable assets upon which one's livelihood and bank account rely. No longer can a few jokes be labeled "innocent" when millions of dollars may ride on the outcome. Even a seemingly small prank, such as changing the value of pi in a single computer, can wreck an entire Ph.D. thesis based upon improper calculations.[33]

Such a change in the system governing commercial airlines or monitors of hospital equipment can cause death or disability. In between the two extremes, there are myriad circumstances in which damage can be inflicted deliberately or by accident to the many millions of operating computers whirring through their daily tasks. So pervasive has become the vulnerability to criminal or roguish behavior that legislative bodies in many countries are revising their criminal and civil laws to make sure that these new transgressions are covered in order to facilitate the curbing of excesses. Indeed, the draft law in the United Kingdom would make "hacking" a crime defined as any "unauthorized access to a computer."[34*]

A review of several examples of miscreant behavior over the last several years will serve to demonstrate the wide range of behavior which is becoming more prevalent, more destructive, and more demanding of legislative attention.

The AIDS Information Diskette[35]

In December of 1989 a disk purporting to be an informational program assisting users to ascertain whether or not they had AIDS was mailed to about 25,000 people from a post office in London. Medical experts who examined the program stated that much of it was quite credible. A

---

*See Preface. Enacted into law July 31, 1990.

warning on the label cautioned that the disk should not be used without dispatching payment to a return address in Panama City. Users booting the disk a number of times were rewarded for their efforts with names of files on their hard disk deleted from the computer's core memory, thus disabling the system that harbored it.

At an estimated cost of $3.00 per disk, plus the cost of packaging and mailing, this caper was not the work of a prankster. Nor was it necessarily a terrorist, as many suspected. According to the lawyer for the person apprehended as responsible, the effort was conceived by an entrepreneur attempting to secure payment for this rather unusual way of distributing his product.

The person in custody was apprehended in Cleveland, Ohio, on a warrant issued by Scotland Yard. U.S. investigators are cooperating with their British counterparts to determine whether and where fraud or other prosecutable behavior took place. The perpetrator is an American citizen, a Ph.D. anthropologist, who has served as a consultant to the World Health Organization. His defending attorney announced that no crime had been committed as his client was legitimately offering a marketable disk for which he hoped to raise money for funding more research on AIDS.[36]

Other Incidents

The episode of the AIDS virus is only one of several that have attracted public attention in recent months.[37] The Internet worm disabled approximately ten percent of the 62,000 computers linked together through a loose collection of gateways to different facilities throughout the country on the night of November 2, 1988, and the two days following. A young Cornell first-year graduate student, Robert T. Morris, Jr., called by one of his Harvard professors the second brightest computer science student he had ever taught, was convicted of felonious behavior in early January of 1990 under the Computer Fraud and Abuse Act of 1986. Morris has now been fined $10,000, put on probation

for three years and will be required to serve 400 hours of community service.[38] After several weeks of thoughtful deliberation, the Department of Justice decided not to appeal the sentence, although there were many proponents of a jail term in order to impress upon would-be rogues that such irresponsible behavior by computer users would not be tolerated.

In March of 1990 two of the three "Hannover Hackers" (one committed suicide) were sentenced in West Germany for unlawful entry into a number of United States databases. They were allegedly seeking secret data from sensitive on-line U.S. databases to sell to the KGB. However, what they took had little value to the West Germans, so the judge let them off with a rather short period of probation. The legal obstacle was that West Germany had no law that would protect U.S. information.[39]

Another recent incident involved the WANK virus (Worms Against Nuclear Killers), whose message appeared on the screens of many NASA computers shortly before the shuttle launch in October 1989.[40] Congressmen attending a hearing shortly thereafter were appalled that one year after the Internet incident, NASA's computers were still open to such obvious penetration, even though the intent of the invaders was merely to attract the media to their political protest not destruction. Some suggested the need of a "computer Czar" (the term actually used) who would assume some centralized responsibility for bringing the level of security throughout the country's computer networks to some level of acceptable impenetrability.[41]

These several episodes threaten the exercise of proprietary rights over information and have deleterious consequences for a highly computerized environment. The Internet worm was "let loose" intentionally by a bright but perhaps misguided student without any proven malicious intent but with the alleged desire to demonstrate weaknesses in the Internet system. The Hannover Hackers were seeking entry into secure systems, in order to sell information for profit, not for political motivation. On the other hand, the designers of the WANK

virus although politically motivated, only wanted to attract publicity for their views, without any deleterious consequences, as no data were reported to have been destroyed or damaged.

From the above examples, it is possible to conclude that the variety of miscreant behavior affecting proprietary or privacy rights in information can be quite varied and complex involving many jurisdictions and many different types of behavior. The attitudes toward such behavior can also be quite varied. Law enforcement officials seek harsh punishment, whereas software programmers tend to be more lenient. They come from a professional ethic which tolerated a fair amount of experimentation as a methodology for cutting computer teeth in a new and unexplored environment.

Much of the behavior is deleterious – but perhaps not intentionally so. Often terrorism is suspected. If so, there have been no claims of success made by terrorist groups. Extortion, but to what end? Perhaps an effort to protect intellectual property and ensure proper compensation, but, if so, quite misguided and mischievous in the extreme. More often the intrusions are carefully crafted and cunningly executed attempts at embezzlement by insiders familiar with the protocols for access and manipulation of the data.[42] For whatever reason, computer pranks, pilfering of data, deliberate distortion of programs, voyeurism in private databases, and other questionable manipulations of data in transit or storage continue unabated.

The AIDS diskette highlights many of the attributes of the newer transgressions. It was transnational, mailed from the United Kingdom to many countries to recipients who themselves have access to many transnational networks. It was global in impact, involving many jurisdictions. The United Kingdom and Panama were primary locations but repercussions were felt as far away as Zimbabwe and Thailand. It is not entirely clear which country's laws were transgressed or which courts have jurisdiction over which parties to the transaction. The issuing company's alleged origin is a country whose flag has been used for

convenience in shipping because of the leniency of its regulatory laws. Panama may have been especially selected as a "data haven."

Tracking down the miscreants required the cooperation of many people in many countries, including both affected company personnel and public safety officials. The cooperation of many law enforcement officers will be required to bring the miscreants to justice. The problem of protecting the integrity of computer networks through which information flows with such rapidity and ease is not a simple task and will require global cooperation.[43]

Without special criminal and/or civil laws clarifying, it is questionable whether or not laws protecting "property" can be applied to pursue takers of information supplied in electronic impulses or disruption of the delivery thereof.

Criminal Prosecution for Malevolent and Miscreant Behavior

The perpetrators of all these incidents are or could have been subject to criminal indictment under current U.S. laws. However, opinion has been divided on how rigorous the prosecution should be. Many observers have faulted the American judicial system for being overly harsh with Robert T. Morris, Jr., although an equal number thought it was important to send a strong message that such aberrant behavior would no longer be tolerated.

Nonetheless, there has been a certain amount of soul searching on the appropriate sanctions to be applied in order to curtail miscreant behavior and also to recompense injured parties. Sending some of the best and brightest computer programmers to jail, as a recent article in the *Harvard Magazine* noted, may not be the optimum path to attracting more students into the profession or building a more competitive and computerized industrial base.[44]

In fact, the federal Department of Justice is cracking down on computer abusers who invade government and business data systems, using the authority they have under the Computer Fraud and Abuse Act, as reaffirmed through the conviction of Robert T. Morris, Jr. All across the country law enforcement agents are busy locating and prosecuting alleged computer miscreants. In some fourteen cities a concerted effort, called Operation Sun Devil, effected the seizure of about 40 personal computers and some 23,000 data disks. Seven operators of computer bulletin boards have been arrested. Others, who have not been charged, have been effectively put out of business through the silencing of their equipment.[45]

Civil libertarians, as well as a number of prominent software designers, are concerned that this amounts to overkill which will severely handicap a tender and vulnerable new industry. Mitchell Kapor, a creator of Lotus 1-2-3, the popular spreadsheet program, has led an effort to raise money for the defense of some of the accused. *Amicus curiae* briefs have been filed by the Electronic Frontier Foundation in support of defendant Craig Neidorf, also known by his electronic alias, "Knight Lightning."[46] According to Mr. Kapor's lawyer, Harvey Silverglade, a civil libertarian from Boston, the Department of Justice is pursuing a "typical American solution: throw your best and brightest in jail."[47]

According to the DOJ, however, the effort has been targeted primarily toward a network of computer "cyberpunks"[48] calling themselves the Legion of Doom, whose members exchange information on techniques for breaking into computer systems on their bulletin boards.[49] Another investigation has been targeted toward a group called Nuprometheus League, after the Greek hero who stole fire from the Gods for the benefit of mankind. Nuprometheus' target has been the basic programming information from Apple computers, knowledge of which is essential to permit other manufacturers to produce Macintosh-like machines.[50] This purported motive is consistent with the philosophical environment in which the gifted young "hackers" (meaning highly skilled tinkerers) shared their intellectual achievements.

However, in the United Kingdom, legislation is being proposed which would define "hacking" as a criminal act.** The essence of "hacking" is obtaining or attempting to obtain unauthorized access to data held in a computer regardless of the intent, whether for deliberate misfeasance or through willful or wanton negligence.[51] In the United States the concern has been more on defining what level of intent or negligence should command what level of punishment. Senator Leahy has introduced into the U.S. Senate an amendment to the Computer Abuse and Fraud Act which would include a transmission which causes damage, disruption, malfunction if caused either by "reckless disregard" for the consequences or by intentional or willful action.[52]

It is not entirely clear yet which sanctions will be effective to punish wrongdoers and to prevent future incidents. Several states are experimenting with innovative practices to curtail such misadventures. These include such imaginative retribution as withholding university degrees, depriving the miscreant from participating in the profession for which he or she is qualified, as well as confiscating computer equipment used for the unacceptable behavior. A member of the Public Utility Commission of New York has even proposed withdrawing telephone privileges from users who commit computer transgressions, a rather stringent sanction considering the indispensable and pervasive character of telephone service in today's world.[53] However, all of these are controversial practices, and it is not yet apparent what will be considered appropriate or efficacious.[54]

**See Preface for U.K. statute.

CHAPTER THREE

OWNERSHIP OF FEDERALLY GENERATED INFORMATION RESOURCES

In the United States, information policies dating back to the nineteenth century, when the country was largely agricultural, dictated that information funded by federal sources should be available to all and the property of none.[55] Section 105 of the Copyright Act so limits federally generated information products,[56] which would otherwise be copyrightable. This policy was eminently sensible and justifiable in a country which was largely self-contained economically, with a predominant but highly disaggregated agricultural base. It meant that research data gathered and analyzed by the federal government would be distributed widely to farmers nationwide with no strings attached. The benefits were apparent to all and questioned by few. The natural consequence of such policy, however, is that the information flows freely and without compensation not only to one's own countrymen but also to competitor countrymen as well: A generous but perhaps not entirely successful information policy for a highly competitive industrial or information-based global economy.

Interestingly enough no such prohibition was instated with respect to the patent law. In recent years government patents have been made available for transfer with proprietary rights to the private sector.[57] This has been accomplished to expedite the commercial exploitation of many products and processes which were languishing unused for the lack of legal tools with which to protect and reward investment in the commercial development of such patent rights.

Section 105 has been largely overlooked until recent agitation has erupted urging its modification to encourage such transferability of copyrightable materials to private sector entrepreneurs. The Register of Copyrights issued a report in 1961 suggesting that the power to make exceptions be given to that office,[58] yet the matter was handled only cursorily during the debates prior to the 1976 revision of the Copyright Act. However, in 1976 it was thought that the number of exceptions

would be few and instances of actual benefit to the public would be rare.[59]

Today just the opposite view is being urged, that the benefits are obvious and the detriments few.[60] The arguments concerning the benefits revolve primarily around computer software as an asset which is commercially viable. According to the current Register of Copyrights "these works have a certain functional, or utilitarian aspect about them which some argue differentiates them from the more traditional copyrightable works, such as books and paintings. It may be time for a change."[61]

Federal Agencies (such as DOD, USDA, NIST, and NASA) spend millions developing computer-based training materials and other useful software, which have potential commercial value. Administrators of these agencies regret their incapacity to enter into cooperative joint ventures with the private sector to market their intellectual products. Both large and small firms in the private sector bemoan the inhibitions inherent in the current legal environment which discourage them from utilizing and marketing government generated software packages.

For example, Nielsen Engineering & Research, Inc. (NEAR), a small research company based in Silicon Valley, California, told a congressional committee in April of 1990 that its attempts to acquire maintenance rights to two software packages for missile aerodynamics, named SWINT & ZEUS, failed because the federal agency responsible for developing the software had no incentive to implement an agreement for technology transfer and had no proprietary rights to transfer leaving NEAR with no exclusivity to protect its investment in maintaining and marketing the software. As a consequence, the U.S., which has been a world leader in aerodynamics research, is lagging behind European firms. As the United States is the world's largest producer of software, a substantial proportion of which is generated in government facilities, this failure to offer an incentive to transfer such technological breakthroughs to the private sector for exploitation represents a major

crack in the legal dike which supports software development for the world market.

The General Patent Counsel of Martin Marietta Energy Systems, Inc. further testified that "a significant amount of potentially valuable software," developed in its Oak Ridge facilities, "could be licensed for use in the private sector" if appropriately protected "through a proper intellectual property right." Government regulations, which require wide-spread dissemination of knowledge about computer software generated under government funding have a negative impact because "what is free to everyone will be invested in by no one. Also what is free to everyone in this country ultimately means it is free to everyone in every country."[62]

A research psychologist for the Army expressed frustration over the failure to market to the general public computer-aided training programs developed by Army specialists. "Relatively little effort would be required to customize JSEP [Job Skills Education Program] to serve the unique needs of such disparate constituencies as English as a second language, the handicapped, the elderly, displaced homemakers, disadvantaged youth, prisoners, or welfare recipients," indeed, to "become the standard for improving job-related performance skills, possibly serving as many as 25 million users."

Software placed in the public domain languishes unused, because "contemporary users have grown accustomed to reliable software support and other amenities such as a toll-free number to call when problems arise" which support system government agencies are not funded or authorized to provide. The optimum transfer of federally developed technology and beneficial development by and for the private sector will not take place "until the Government obtains unambiguous, transferable intellectual property rights that cover software."[63]

With the candor and force of such testimonials prompt legislative response would seem inevitable. Not so, however, as there are powerful forces opposing any change in Section 105. The Information Industry

Association, with considerable lobbying clout, reminds legislators that it has been a long-standing policy of the federal government to expedite the distribution of government-generated information.* Many members of the association rely heavily upon government sources for the raw material of their publishing arms, in both print and databased form. As a consequence, they fear increased costs of operating if they find it necessary to enter into joint agreements with their government agency sources and/or to pay royalties back to the hands that feed them.

Thus any legislative initiative will likely have to differentiate between government source computer software and government source print and data content if any reforms in the current wording of Section 105 are to be realized. It is not clear either whether or not the appropriate strategy is to amend Section 105 or to append special privileges for computer software through amendments to the Federal Technology Transfer Act. As substantial administrative turf is at stake, administrative agencies will also need placating if they lose control over jurisdictional territory.

---

*In July 1990, the IIA Board of Directors issued a policy statement reaffirming support of a citizen right of access to government source information "regardless of the media in which it exists."

CHAPTER FOUR

TRIPS IN THE URUGUAY ROUND

The U.S. Special Trade Representative, Carla Hills, had tabled in mid-May of 1990 a proposal to create an international system for the protection of intellectual property rights within the GATT. The Draft Agreement on the Trade-Related Aspects of Intellectual Property Rights is popularly known as TRIPS. The Uruguay Round of discussions has bogged down on a number of issues, most especially the agricultural ones, but Carla Hills has stated categorically, "without a successful agreement on TRIPS, there can be no successful Uruguay Round."[64]

Such determination is the result of frustration with existing international legal regimes for the protection of rights. The protection of such newly emerging technologies as computer software, databases, and semi-conductor chips is being incorporated into existing legal structures worldwide at a snail's pace compared with the march of the marketplace. With the United States a leading producer in all three areas, it is not surprising to see U.S leaders gnashing their teeth. However, as the Japanese and other even smaller countries proceed inexorably to excel in these areas, such strong protection may not always be in the best interest of the U.S.

Nonetheless, the U.S. is pushing for a centralized system, at least among the powerful trading nations which will better protect what are essentially the crown jewels of the information age.[65] The proposal purports to harmonize the trading environment by establishing minimum levels of protection and by providing for generally recognized principles for enforcing both existing and newly created rights.

Countries entering into the agreement would provide protection no less than that provided in the Paris Convention on Industrial Property (Stockholm 1967) and the Berne Convention for the Protection of Literary and Artistic Works (Paris 1971). They would agree to "national treatment" no less favorable to importers than afforded nationals. They would initiate due process by means of civil, criminal, and/or

administrative law which should "not be unnecessarily complicated, costly, or time consuming" and provide an opportunity for judicial review.

Most significant is the requirement that contracting states provide protection for trade secrets, a practice which is common in the United States for computer software but not honored in many other trading nations of the world. The tabled proposed annex, Article 31, to the GATT would impose a positive obligation to provide an opportunity for natural and legal persons to prevent trade secrets from being disclosed in a manner "contrary to honest commercial practices." However, the article contains rather powerful exceptions "to carry out necessary government functions . . . to protect human health or safety or to protect the environment."

Protected works are to include computer programs, databases, and semi-conductor chips. However, there is a stipulation that the "first sale" doctrine shall not apply to computer programs so as to exhaust the rental right. Buyers of computer programs would not be permitted to set up rental houses without the permission or participation of the rights holder in the commercial advantage to be gained.

For video works, the definition of "public" for the purpose of prohibiting "public performances" without the permission of the rights holder would be specified not to exclude members of the public capable of receiving such communications in diverse locations and at different times from the communication or transmission of the program. Thus a major effort is being put forward to protect the interests of U.S. video producers and software programmers in the world markets. Whether this effort will succeed remains doubtful, as these are the two areas in which piracy of U.S. products has been most rampant. Efforts to reach bilateral agreements have been somewhat successful in a number of the countries with the most flagrant abuses.

CHAPTER FIVE

PRIVATE ALTERNATIVES TO JUDICIAL PROCEDURES: THE IBM/FUJITSU ARBITRATION

Sometimes judicial procedures are not adequate to determine controversies between parties, especially if they come from different nations with disparate legal systems and political attitudes. When Fujitsu took advantage of information (allegedly obtained either without IBM's authorization or consent or exceeding authorizations contained within several licensing agreements) about IBM operating software to design clones which were plug compatible and competitive with the IBM machines, the judicial systems of both countries were bypassed in order to resolve the dispute between the two companies. Perhaps IBM was apprehensive that, even if the American company could obtain a favorable decision within the U.S. judicial system, that it would be fruitless to attempt to collect on the judgment within the Japanese judicial system.

The alternative methodology adopted was to turn to private arbitration which both parties agreed would become binding upon them.[66] Two independent experts were selected by the parties, one a law professor at Stanford University and the other a retired executive of the Norfolk Southern Corporation. The dispute involved whether or not millions of dollars of royalties should be paid to IBM, the largest computer company in the world, by Fujitsu, the largest computer manufacturer in Japan, whose many customers all over the world had come to rely upon operating systems which were compatible with IBM machines. Thus the interests in the outcome exceeded the proprietary or acquisitive interests of either of the two parties and extended to a large body of users with installed equipment.

The decision was probably not optimum for either of the primary parties to the controversy but permitted the users to continue to have access to the IBM software for a long enough period to make accommodations if it were thereafter denied to Fujitsu. It also allowed a period sufficient for Fujitsu to develop alternatives to reliance upon the IBM source.

What transpired was that IBM obtained a declaration of its proprietary interest in the software but Fujitsu won the right to continue selling and servicing its equipment with IBM products incorporated. Fujitsu was ordered to make payments for such privileges in the amount of somewhere between 25 and 50 million dollars annually depending upon the extent of the use. IBM permitted Fujitsu a right of disclosure of its interfaces until June 25, 1997, when IBM would be allowed to operate a secured facility regime excluding Fujitsu thereafter.

For prior access to IBM software, the arbitrators determined the value of a paid-up license fee to be almost 394 million dollars leaving a balance of approximately 237 million dollars due from Fujitsu to permit continued use of the IBM operating system software. The dollar amounts thus determined may have been far in excess of what Fujitsu hoped – a decision determining that operating systems software should be accessible and in the public domain. However, under U.S. law such access is normally not available unless an antitrust case can be supported showing that the company has used its dominant position in a market to exercise monopoly powers in a predatory manner.

What Fujitsu gained from the arbitration procedure was access for a substantial period and insulation from any future claims by IBM against Fujitsu for infringement of intellectual property, at least concerning the operating systems software which was the subject of the arbitration procedure.

Although, in retrospect, IBM executives may feel that IBM came out the loser, there were substantial benefits looking from the perspective of making the prior decision to use the U.S. courts or to seek alternative measures. In the absence of established and reliable legal precedent upon which the company could rely to protect its interface standards from mandatory disclosure, and the concern that the judges would not have adequate background to understand the issues, the ability to participate in the selection of experts familiar with the industry would appear to be quite advantageous.

One is reminded of Winston Churchill's popular commentary on democracy being a most difficult form of government but the best considering the alternatives. As joint ventures between companies with different nationalities become more the standard than the exception and as piracy and misappropriation of information become more rampant, national judicial systems are strained to accommodate inconsistencies in national laws and policies. Assets which some consider private property, others consider to be in the public domain. Given the choices, it seems apparent that arbitration procedures may come to be relied upon rather more than less in the future.

Only a reliable international legal system, to which all parties adhere, will provide an opportunity to settle disputes in a more structured environment. Such a legal regime is only remotely extant in the international arena, since the intellectual property laws are only in a modest sense harmonized within such international institutions as the World Intellectual Property Organization, the rules of trade in manufactured products within the General Agreement on Tariffs and Trade, and the information transport rules within the International Telecommunications Union. Indeed, the latter union, with the longest history of international cooperation, has enjoyed considerable success in reaching agreements on standards governing the interoperability of telecommunications systems. However, the success is bound inextricably with a system of government monopoly operated telecommunications systems in most of the countries of the world, only a few of which have recently been experimenting with privatization of facilities within their own countries. This system too will be strained as privatization continues at its current pace. With its multiplicity of carriers of differing levels, size, and service competing both domestically and in the global market, it seems clear that efforts to harmonize the legal systems need to proceed at a similar pace.

CHAPTER SIX

THE VIDEO MARKETPLACE: RECONCILING PIRACY, PROFIT, AND PRIVATION

The impact of new technologies on property rights in information has never been more complex or controversial than in the video marketplace. Consider the advent of the following technologies, each of which has presented new challenges to the legal system:

- Cable television, which could deliver broadcast signals to distant locations,
- Videocassette recorders, which could archive television programs for personal libraries,
- Computer graphics, which can revamp reality to entirely different configurations,
- Satellite dish antennas, which capture signals from the air.

Cable Television

Early on the Supreme Court had great difficulty in deciding whether or not a cable system was merely enhancing the ability of the viewer to receive a broadcast signal or delivering an entirely new rendition for which compensation should be paid. It came down on the side of the cable customer who badly needed the enhanced signal to clear the snow from the television screen.[67] However, when distant signals were imported by microwave, the FCC developed elaborate rules for how many signals could be imported into what sized communities.[68] Eventually a compromise was reached whereby the cable television systems were required to pay some adjudicated fees for the program which they took from the broadcast sources but were accorded a compulsory license which legitimized the taking. At the same time the Federal Communications Commission assured protection of local broadcasters by requiring mandatory carriage ("must carry") of all broadcast signals available without enhancement within a 35-mile radius of the cable system headend.[69]

However, the marketplace moved forward with more and more cable programming entries vying for access to the limited number of channels available for distribution, especially on the older 12-channel systems. Finally, Ted Turner grew impatient, and sought court action to have the "must carry" rules declared unconstitutional. These and a subsequent set of "must carry" rules have been set aside.[70] However, the courts have not declared a "must carry" provision impossible to devise. Therefore, efforts have been turned toward Congress to write some form of "must carry" requirement into the Communications Act.

Notwithstanding such efforts, the cable industry relishes a time in the not too distant future when a "must pay" rule might come into being to assure access to the delivery channels offered by the cable television industry. However, the telephone companies, having been forbidden from entering this market, wait impatiently to be let into the competition which could forestall any regulatory requirements on what either the broadcast or cable delivery system might offer the customer in video and/or data services.

The telephone companies seem to be looking more toward the latter than the former as a more doable relaxation of rules prohibiting them from full competition within the new information marketplace. Already Judge Greene has ruled that telephone companies may provide a gateway for information services to be provided by others but may not become information providers themselves,** and AT&T has survived the seven-year ban on its entry into electronic publishing.

**In July 1991 Judge Greene lifted the judicially imposed prohibition against providing information services, leaving the RBOC's free to compete in the data market. This ruling leaves undisturbed the statutory restriction against direct competition with cable companies in their service areas, moving the agitation for repeal to the legislative arena. U.S.A. v. Western Electric Co., Inc. et al., U.S.D.C., D.C., No. 82-0192, July 25, 1991, 3 CCH Computer Cases ¶46,489 at 63,262.

Backyard Satellite Antennas

The marketplace also ran ahead of the law with the advent of backyard satellite dish antennas. The cable television signals, which they received, were not "public" signals, since they were being delivered to cable television systems for redistribution via underground cables. Broadcast signals were legally available for the taking by anyone within reach of the signal. Section 605 of the Communications Act[71] had not been clarified to prevent backyard dishes from picking up the unencrypted signals, although the legality remained in a murky cloud of confusion. This did not prevent the sale of a large number of antennas to eager buyers who wished to receive the many new programming services delivered via satellite beginning in the mid-seventies.

Indeed, by the time the 1984 Cable Television Act[72] was written, it had become apparent that a lobby of one million or more installed antennas was a formidable political force despite the finding of the Federal Communications Commission that reception by such users was unlawful.[73] The new Act clarified the situation with respect to access to satellite-delivered signals stating that anyone with the technological capability could legally receive such signals unless they were offered through a marketing scheme in which the consumer had enjoyed some bargaining position.[74] As a consequence most of the subscription services went to encryption almost immediately, and over time the majority of the more attractive signals (even three of the four public broadcasting signals and including network feeds to their affiliate broadcasters) became encrypted also.

Moreover, Congress acted to regularize the access for antenna owners to subscribe to satellite-delivered programming services and for a compulsory license both permitting the service and requiring royalties to be paid to the producers.[75] In this way the interests of an estimated 22 million rural households were reconciled with competing interests of the cable companies which have come to enjoy a symbiotic relationship. Although cable passes 80 percent of the television homes in the United States today, there remains a full 20 percent which cable

is unable to serve other than through a satellite-delivered service directly to the home.

Video Cassette Recorders

Likewise, the challenge of Universal City Studios to Sony Corporation's Betamax videorecorder did not reach the Supreme Court, with its pursuit of compensation for programmers delivering television video product to the home consumer, until after the marketplace had made its own decision about videorecording. Although the lower court had found a copyright infringement from videotaping television programs, the justices, understanding the limitations of their judicial sanctions, decided that there existed a personal right to tape video product for later viewing. They drew the line at such "personal use" only, conceding no commercial right of entrepreneurs to market such taped broadcasts for their own profit.[76]

To have held otherwise would have required a police state to enforce the prohibition. In fact, the Royal Canadian Mounted Police did destroy satellite antennas in Canada until they met with the strong objection of loggers who were unable to receive television signals otherwise in their remote workplaces. Thus the law has groped slowly in the direction of a viable compromise between the practicalities of coping with the new potential for delivery of video signals while preserving some remnant of equity, as well as profit, for the producers of the video services.

Rental Rights

The marketplace has not always favored the information providers. The "first sale" doctrine of the Copyright Act prevents a seller of a book, for example, from controlling the subsequent use or sale.[77] The provision served the library community and its users well during a print dominated era. However, the change from movie theaters as the predominant mode of motion picture delivery to videocassette rentals

excluded the motion picture producers from collecting rents from the videocassette viewer after the sale of the cassettes to the retail distributor.

The "first sale" doctrine is also a worrisome problem for producers of computer software, who have devised a "shrink-wrap license" that purports to avoid the transaction from being characterized as a sale, thus permitting the prohibition of rentals without the consent of the manufacturer or copyright owners. The use of the "shrink wrap" license is a questionable practice, not yet approved by the courts, and specifically rejected by the recommendations of the European Community. However, Congress has yet to pass legislation favored by the software industry to prohibit the rentals of computer software without the specific agreement of the copyright owners.[78*] Efforts to reform the applicability of the "first sale" doctrine are a contentious issue for librarians who continue to lobby for an exception to any prohibition for "loans" of such public institutions.

Colorization of Old Movies

Another area of concern has been the ability of the computer to transform video product into different configurations. The primary area in which this has come up in recent months was with respect to the colorization of old movies, which many producers and actors as well as movie devotees felt mutilated the video product and desecrated the sanctity of the intellectual creator's product. Famous actors, such as Jimmy Stewart and Burt Lancaster, along with producers George Lucas and Steven Spielberg, descended upon Washington to lobby their Congressmen to protect the original works of art as conceived by their producers and actors – a right known in Europe as "moral rights."[79] What resulted was a compromise dictated by the demands of marketplace economics with the result that a number of motion pictures have been designated "classics"

---

*See Preface for passage of amendment to require authorization of rentals.

which can only be shown as such in their black and white of their original release.[80]

However, the demands of the marketplace once again won the day with colorization rampant among many of the older movies in order to capture the attention of the younger viewers who do not remember the "oldies" without color. The Copyright Office, in fact, will register the colorized version as a new copyrighted work, which means, as a practical matter, that a copyright owner with black and white inventory can extend the life of the copyright of product far beyond the original time period authorized by the Copyright Act.[81]

Computer Enhancement

What will happen with the ability of computers to replicate, revamp, and meld together bits and pieces of video information from many sources remains a mystery. *The National Geographic*'s use of a picture of the pyramids moved closer together than reality brought an army of dissent to this mutilation of nature.[82] Bette Midler, obtained an injunction to prevent the use of a mimic of her voice on a television spot advertising a company for which she had refused to record the music herself.[83] This is certainly an area to watch in the future, as entrepreneurs seek to push the limits of the technology in bringing together new product devised from old.[84] Moreover, it will tax the best legal minds to come up with practical solutions to the allocation of compensation for use of video as well as data product.

Electronic Publishing

Electronic publishing of data is still in a volatile environment both legally and economically. No one service has yet proved its value as a general purpose information utility or consumer-oriented service to all customers. The niche services delivered to home and business computers continue to draw a steady if slow flow of new customers for such

services as LEXIS for lawyers, Dow Jones Information Services for the financial markets, OAG for airline information, BRS for librarians, and Dialog for scientists and engineers.

It is with these services that some of the more interesting legal cases have arisen. For example, West Publishing sued Mead Data, the provider of LEXIS, for copyright infringement claiming a proprietary right in the page numbers cited in West volumes, in which are published many of the official court decisions. Conceding that keywords and other annotations were the property of West, Mead claimed the public interest in compatibility and clarity of references for all lawyers required use of similar page numbers. The case was settled before a final determination was reached, but Mead has initiated its own system of citation of the LEXIS data, as much of its content actually precedes access to the West published works.[85]

With the advent of "hypertext" and "hypermedia," which combine segments of text with both video images, the question of allocation of legal rights to recompense will become intense. The archiving of photographs is severely inhibited by the difficulty of obtaining rights from a large number of photographers, and some form of compulsory licensing, which is another way of declaring a public domain, may become necessary if the advantages of these new methods of disseminating information are to flourish.

CHAPTER SEVEN

COMPUTER SOFTWARE PROTECTION IN THE EUROPEAN COMMUNITY*

A controversial proposal on the protection of computer software has emerged in the European Community.[86] Whether or to what extent computer software should be covered by existing copyright, patent, or trade secret laws has been a source of great controversy in most developed nations for the last decade. Many countries have adopted the now predominant view that copyright protection is more appropriate than patent law. There are some strongly opinionated proponents of the view that patent law would be better, because it is the idea rather than the embodiment of the idea which is most innovative and needs protecting in software.

Proponents of the copyright alternative argue that it may be the idea which needs to become available to copy in order to encourage uniformity and conformance for user convenience. Some mavericks suggest that some combination of copyright and patent and/or trade secret laws could make a better match for what appears to be quite utilitarian (which has been considered the province of patent law) and not appropriate for copyright (which is "literary and artistic expression"), but expended through a faster life cycle than seems optimum for pursuing a patent.[87] Most countries which have addressed the problem have gone the way of enacting laws to extend copyright coverage to software, and that is the major thrust of the EC directive.

What is most controversial about the directive is the nature of the restraints on reverse engineering or decompilation of the underlying code in order to study its function and to learn how to build a better mousetrap. The concept is borrowed from patent law where taking apart a machine to understand how it works is not forbidden. What is forbidden is to build the same machine or employ the same process without receiving permission from and offering compensation to the creator.

---

*See Preface for later version of directive as enacted.

Reverse engineering[88] is, therefore, a concept alien to the copyright law where the product (usually a manuscript, painting, video product, sculpture, musical composition, or map) is open and available for viewing. What is prohibited is "copying" of the particular expression not "use" of the underlying idea.

The controversy has pitted the Americans (not all, but a majority) against the Japanese. The Americans look upon "reverse engineering" as a license to pirate their proprietary software, whereas the Japanese look upon "reverse engineering" as a protected right of cloners who wish to produce plug compatible, interoperable, and interchangeable software for use in the same or similar machines. This is reputed to benefit consumers by providing a larger selection of choices at lower costs.[89]

The ambivalence with which intellectual property laws were enacted suggests that a primary purpose of the statutes is to encourage the dissemination of knowledge and transfer of technology to serve the viewing and user public at reasonable costs and only incidentally to offer financial award to creators. According to one view such rewards should not be niggardly but only sufficient to assure a steady input of innovative new products and services as well as literary and artistic works.

Smaller software houses in the United States tend toward the Japanese view as do many European companies for the primary reason that the U.S. dominates the world software market and many third world countries, as well as Europeans, have targeted software as an industry which requires little capital investment and the application primarily of brain power, a good education system, high motivation, and ingenuity – all components over which the United States has no monopoly.

The exact terms of the proposed EC directive are confusing and sometimes contradictory. Rather than setting forth a coherent system of harmonization of the laws of member states, the EC has devised a set of general principles to be followed. This may exacerbate rather than relieve the hodgepodge character of existing intellectual property laws.

For example, the definition of what constitutes "an original work" for the purposes of protection is not uniform among the member states, and the directive makes no attempt at uniformity.

The directive's intention concerning applicability to software interfaces seems somewhat confused. Article 1(3) of the directive states that copyright protection shall not be given by member states to the "ideas, principles, or logic which underlie the program. . . ." Neither would the algorithms be capable of copyright protection, although in exceptional circumstances they have been capable of capturing a patent. Thus having taken a strong stance in favor of interoperable computer systems and open interconnection between different pieces of software, the directive seems to contradict this benefit by adding in Article 4 that no reproduction or adaptation of a computer program will be permitted by any means. This seems to require the consent of the copyright owner to make any effort to understand the underlying structure in order to assure compatibility.

On the other hand, Article 4 prohibits restrictions against users made by the copyright owners on software packages which are not made available under an agreement signed by both parties. Article 5 specifically permits users to make use of the software on any equipment at any location and to modify the program for their own uses even if this involves reverse engineering or reverse analysis. This is presumably designed to cover the "shrink-wrap" licenses used by most software companies marketing to the consumer market to get around the "first sale" rule which prohibits the copyright owner from controlling the use of the product beyond the first purchase. According to the directive the balance of power between manufacturer and user of mass-marketed software is unequal and the greater power should not be used by creators of software to "circumscribe the normal enjoyment of property by a person who legally acquires a program by purchase." Thus providers who wish to continue to restrict the use of their software would be required to obtain the written agreement of the purchaser in order to convert them legally into a "licensee."

Creators of software and manufacturers which control large operating systems are strongly opposed to any reverse analysis arguing that decompilation is not necessary to promote interconnectivity. Rather they assert that the marketplace is a far better environment in which to develop interconnectivity. Software providers, they suggest, find it in their self-interest to provide compatibility of systems software and operating software, as well as ease of network interfaces and transferability of information from one manufacturer's hardware to another. In any event, they see the antitrust laws as providing adequate protection against any predatory behavior.[90]

The exclusion of software "interfaces" especially without an accompanying definition, is strongly opposed by most major manufacturers in the United States. A group of congressmen wrote to Secretary of Commerce Mosbacher in March of 1990 that legalizing decompilation and prohibiting protection of interfaces would severely deter U.S. producers as "Decompilation only helps copiers advance their own competitive interests at the expense of the original developer. . . ." Thus, "The American software and computer industries will be severely damaged by a successful attack on the copyright protection afforded interfaces in computer programs."[91]

Article 1 (4b) specifically incorporates machine generated software as copyrightable by the humans responsible for the creative effort leading to the machine-generated "original works" or to the "natural person or persons who have created the work, [Article 2(1)] or "the person who uses such a tool to generate programs should be considered as the creator of those programs" even though the human "author" may have little value or only a modest contribution to the output of the intelligent machine [Article 2 (5)].

CHAPTER EIGHT

AUTOMATIC NUMBER IDENTIFICATION

Privacy is a quest for many users of telecommunications systems, just as publicity is equally a quest for many others.[92] How to reconcile these two divergent desires leads to an almost insoluble conundrum. At one end of the spectrum are those who wish to be left alone and not disturbed electronically or otherwise. The New York Telephone Company has found that 34 percent of its customers in Manhattan and 24 percent statewide require unpublished telephone numbers with numbers as high as 55 percent reported requesting an unlisted number in California. On the other hand direct mail merchandisers desire to obtain telephone numbers from all prospective customers especially those with high order rates. Indeed, telephone companies have engaged in a practice of selling those telephone numbers which call 800 and 900 numbers to the companies subscribing to these services.[93]

Into this tug-of-war has come the technological miracle of "automated number identification"(ANI) to delight some and confound others.[94] Direct mail merchandisers, as well as small entrepreneurs who do not have fully monitored telephone service find it a technological blessing to be able to obtain this information automatically without requesting the customer to divulge the number. However, many customers of American Express were spooked by company representatives who answered their calls giving the name of the caller, pulled up from a computer by the telephone calling number.[95] Others considered it an invasion of privacy and have lobbied to have the service prohibited.

There is no simple solution to the dilemma confronting telecommunications service providers, for they cannot satisfy all customers. An ANI service has been authorized in Maryland since October 1989 and in West Virginia and Virginia since November 1989.[96] However, the Pennsylvania Public Utilities Commission recently was ordered by the courts to stay execution of its authorization pending a satisfactory solution to user option on releasing the customer's telephone number.[97] Bell Canada, on the other hand, has been authorized to offer "Caller ID"

so long as operator-assisted blocking of the number identification is available on a pay-per-call basis. This is intended to encourage use of the number identification requiring the caller to "have a strong need for anonymity" if such service is to be curtailed.[98]

In New Jersey, where the service has been offered for several years on a limited basis, the phone company reports a marked drop-off in obscene and annoying phone calls. On the other hand, police officers claim that anonymity is a prerequisite in receiving tips, and social workers want insulation from being disturbed at their home phones by their disturbed and sometimes violent patients. There have also appeared complaints about the protests written by outraged citizens in opposition to Caller ID, because these telephone customers considered ANI a desirable service which can permit the customer to avoid unwanted callers of all kinds.[99]

A recent survey found a modest majority of the public (55 percent) in favor of telephone companies offering caller identification to those willing to pay for the service.[100]

CHAPTER NINE

MARKETING OF CONSUMER-ORIENTED PERSONAL DATA

The more difficult question is the value of personal data such as the telephone number, name, and address, all of which can be provided electronically by a reverse directory, which many direct mail houses are organizing for their own internal use. The public in general believes that too much information is being collected, control over it has been lost, and the law does not offer sufficient protection.[101]

If personal information has value for commercial purposes, is not the source (e.g., the individual from whom the information emanates) as well as the custodian (the party in whose database the information is archived) entitled to some compensation if the information is divulged to third parties for commercial use? Indeed, shouldn't the individual be entitled to know whereof use of personally identifiable information is to be made and for what purposes, and, furthermore, be entitled to forbid or lease entitlement to such uses?

The Cable Communications Act of 1984 was a major step forward in assuring cable customers the right to be informed of information collected about them and its intended use, and to be given an opportunity to refuse the collection or release of this information by the cable company.[102] Subsequent to the disclosure that the videocassette rentals of a Supreme Court nominee had been disclosed, Congress moved rapidly to impose a similar prohibition on videocassette rental houses.[103]

This is a small chip at a very large problem which is only beginning to be perceived by the public.[104] The amount of personal data collected by credit card companies is enormous, its value to merchandisers quite considerable, and its current use quite extensive. For example, Porsche has targeted 300,000 Americans with minimum incomes of $100,000 as most likely to spend $75,000 on a new Porsche. But this was only for starters. In a letter designed to appeal to the recipient's profession,

current automobile, location, and personal tastes, the company hopes to attract more customers for its lagging sales.[105]

An enterprising *Wall Street Journal* reporter saved her junk mail for four months to track the onslaught of computer generated solicitations directed to particular tastes. Using various combinations of her name, she generated special catalog mailings for "organic gardening," "corporate stress," "slightly imperfect panty hose" by virtue of the magazines to which she subscribed. The average household receives some fifty-odd catalogs a year, and more affluent households are inundated.[106]

The renting of names which are segmented by market interest has become a well-oiled industry, with charges based upon the value of the names and addresses to the company purchasing. For example, Hugo Dunhill Mailing Lists, Inc. of New York, offers 48,526 buyers of outdoor boots, while Hal L. Burnett recommended the purchasers of L'Eggs Queensize panty hose to a marketer who wanted access to "fat women."[107] Indeed, a Filipino domestic servant in the 10504 area code who purchased a $5.00 ring from a catalog, received, as a consequence, a letter from Ronald Reagan thanking her for her vote (which she could not, of course, have cast!) and seeking financial contributions to secure a Republican Congress. So much for the census data matched with purchases of residents in a Republican-dominated community.

According to Consumer Reports, there are tremendous advantages to such computer-generated marketing information, as it permits advertising to be delivered only to those homes which desire the information:

> As the power of the computers grows, so does the ability to make this form of 'direct marketing' even more directly targeted. Your name probably already appears on a number of mailing lists, which might distinguish you by your age and sex, your income, whether you own your home or rent, what credit cards you have and how often you use them, how many cars you drive, and so forth. Using computers to combine the information on these detailed lists, mail-order companies can compile a portrait of your interests, income, and spending habits. The company can then mail its catalog to those who fit the mold of its target customer.[108]

The correlation of census data with motor vehicle licenses, with credit card purchases, and with contributions can paint a rather accurate profile of most active customers. The only way to avoid the onslaught of direct mail generated by such knowledge is to be a miser, never travel, and pay for everything with cash. If ANI comes about as an ubiquitous service, one can add: to call only from pay telephones.

However, annoyance with the system does not seem to add up to political agitation for its demise. Although more than half claim to be overwhelmed by solicitations, a 75 percent majority admitted making a purchase within the last six months. In Europe, where marketing is much less dependent upon such direct mail solicitation, the Council of Europe has issued guidelines which purport to determine the extent to which personal information can be recorded:

> Any person should be able, where appropriate, either to refuse to allow data concerning him to be recorded on marketing lists; or to refuse to allow data contained in such lists to be transmitted to third parties; or unconditionally and on request to have such data erased or removed from several or all the lists held by users. In addition, any person should be able to obtain and rectify data concerning him which are contained on a direct marketing list or marketing file.[109]

A model Solicitations Act to regulate charitable solicitations by mail and telephone has been drafted by the National Association of Attorneys General and the National Association of Charity Officials which assures the confidentiality of donor identification. The Direct Mail Association provides a service whereby annoyed recipients of direct mail solicitations may request that their names be deleted from all mailing lists but does not permit specific requests by type. The only legally enforceable way to prevent unsolicited mail is to declare it objectionable under the provisions permitted by the postal laws. These require an allegation that the mail appeals to prurient interests.[110] It is not easy to protest unwanted invasions of what many consider the private domain of the mailbox.

If individuals are to regain control over personal data which fuels an information economy, privacy scholar Alan Westin believes that "some imaginative new concepts of personal information ownership and control" must be developed.[111]

The New York Public Utility Commission is proposing a more integrated look at the privacy interests of telecommunications customers in its proposed notice of inquiry on privacy. An interest in privacy appears to be widely shared (American Express found 90 percent of respondent cardholders thought mailing list practices were not adequately disclosed, 80 percent that permission should be required to release personal information, and over 30 percent that federal legislation should be enacted[112]). The Massachusetts Office of Consumer Affairs reports prize letters and phone solicitations as a major source of irritation.[113]

While concern is increasing, the opportunities for widespread dissemination of information seem also to be proliferating. Cellular telephones do not provide an absolutely secure communications environment. Automatic dialers encourage an unfettered increase in unsolicited telephone calls. At the same time speaker phones increase the audience; picture phones invade the privacy of the physical environment; and passive monitoring devices, such as voice stress analysis, can be administered without the knowledge of the subject. All of these threaten confidentiality, privacy, and peace of mind.

An outcry for the establishment of a legal right to prevent inundation by "junk mail," "junk fax," "junk calls" is not likely to disappear in the foreseeable future. How the courts, the legislative bodies, the providers, and the users are likely to respond to the various arguments pro and con cannot yet be predicted.

CHAPTER TEN

SEEDS OF INFORMATION ASSETS LAW

As the new technologies come on line and need to be incorporated into the existing legal system, the accommodation is irregular and often forced. Many of the seeds of a coherent law of information assets are the natural outgrowth of well-established fields of law. Liability for libelous statements in the print media can be easily translated to an electronic environment. Protection of sensitive information related to national security is not as easily translated to an electronic environment, as the ease of electronic communication on scientific networks outpaces the law of secrecy.

There are many legal concepts which are applicable to information assets:

SECRECY encompasses state secrets, corporate secrets, trade secrets, as well as personal secrets. Whereas the law of state secrets and trade secrets is reasonably well-established, rules of protection for corporate and personal information assets are not so well-established.

PRIVACY covers personal information which an individual does not wish to be disclosed to anyone. The battle raging over automated number identification in various jurisdictions throughout the United States and Canada is indicative of the high level of interest users have in protecting their privacy. Although the law of privacy is fairly well advanced in both Europe and North America,[114] developments are yet at the pioneering stage. Clearly, there are conflicting interests in privacy of caller versus privacy of respondent and these conflicting interests are yet to be accommodated adequately within the statute books.[115] What one person perceives as an unwanted disclosure of proprietary information the other looks upon as a protective device to forestall unwanted intrusions. There are no easy answers to such dilemmas, particularly for the telecommunications service providers who cannot design their systems for every conceivable individual taste.

CONFIDENTIALITY covers information which is disclosed to others with the expectation that it will not be released to third parties. There are several well-established areas of legally protected confidentiality involving professional relationships such as lawyers, doctors, and clergy. Not so well-established are areas of confidentiality related to the disclosure of information for commercial or service-oriented purposes which the recipient may find useful as a commodity. For example, banks, insurance companies, credit card companies, and retail merchandisers accumulate information in the normal course of business which can be aggregated in computer data banks to provide valuable marketing resources for many purposes. The appropriate or acceptable level of personal control over such information has not yet been clearly delineated.

There is also a question of confidentiality within a computer network. One of the more interesting aspects of the SYSOP (systems operators who provide open bulletin boards of computer memory on which outside users are invited to put messages) environment is the open expression it encourages. Yet the controversy raging in Colorado Springs over the mayor's oversight of what his peers thought were private messages suggests that we are a long way yet from categorizing which networks are expected to provide complete confidentiality and which are expected to be open to all comments.

Recently a disillusioned participant in THE WELL, a computer bulletin board operating in the Bay area, simulated a suicide on-line, then deleted all of his prior entries from the computer conference before accomplishing the actuality. His colleagues were appalled not only by the suicide but by the deletion of the data. They argued that the contributions to THE WELL were the property of the user community and not subject to deletion by an individual contributor.[116]

There is yet no consensus on types of computer networks as public or private places. Criteria need to be established to tell the difference.

INTEGRITY protects information assets from mutilation or violation by users or owners other than the creator. The term integrity is superior to "paternity" or "moral rights" which have never enjoyed the respect in the United States accorded in European jurisdictions. However, with computer graphics offering endless opportunities for cutting and pasting images, agitation for a right to protect the integrity of information assets may develop rapidly.

The recent furor over colorization of old movie classics is a good example of the difficulty of protecting the integrity of information products which can be marketed as new products to a new audience through the application of a computerized paint job.

LIABILITY prescribes the standard of care required by providers or users of information in order to assure that innocent parties are not injured by carelessness or negligence.

What standard of care should apply to which types of computer network? What level of responsibility is appropriate or desirable? Who should promulgate the rules? Who should monitor the performance? To what extent is a user expected to "drive defensively?" Whose responsibility is it to authorize use of machine resources and whose responsibility to debug, check for viruses, manage and advise human resources, provide instruction, warnings, testing, management of software protocols, and authorization of gateways? What is the extent of responsibility for misuse by third parties?

Often the damage is in the anticipation rather than the actuality. This was the case with the Aldus Peace Virus which merely displayed an innocent and benign peace message on thousands of Macintosh computer screens on March 2, 1988.[117] Substantial costs ensued from this otherwise nondeleterious virus, as software houses whose disks were contaminated, or thought they might be contaminated, experienced considerable anguish and expense in examining their inventory for evidence of the virus.

Should manufacturers of computer equipment, software providers, and designers of network architecture be held strictly responsible for delivering an error-free product to the public? Should they be held to the highest standards of care in providing their products to the public or should the policy be *caveat emptor*? Software designers are in agreement that there is no such thing as a bug-free program. Corrections, updates, and improvements are the rule rather than the exception. If software manufacturers were required to recall every piece of buggy software, as automobile manufacturers are required to recall dangerous equipment, they would soon go out of business. Thus the software industry looks upon strict liability as a threat of extinction. However, there may be some uses of software which can cause such unacceptable consequences as to trigger a need for strict liability in such cases.

ACCURACY confers a right to ensure that information which is distributed may be corrected by the subject covered. Such right is established by law for many jurisdictions applying privacy laws to publicly held databases and has enjoyed limited recognition in the law of broadcasting. Although Congress has enacted a right to reply to personal attacks,[118] the Supreme Court found unconstitutional a Florida statute which purported to establish a similar right of reply for newspapers.[119]

REPLICABILITY (called "fair use" in the copyright realm) is a developing area which establishes what is fair and reasonable for a user, lessee, or purchaser to copy or use without compensating the owner of the information for such replication. The arguments over user interfaces and "reverse engineering" are essentially arguments over the fairness and necessity of copying the information products of others in the interest of providing better access, healthy competition, and ease of use of compatible programs.

ACCESSIBILITY is a claimed right to assure access to information which is considered in the public interest to be distributed widely to

the entire population.[120] The legal right can be applied to information technology as well as to information content.

SECURITY implies a robust and functioning system which is not subject to disruption or impairment. The utility of the information highways lies in ease of interconnection. Thus designing a "safe" computer network environment means compromising security in the interests of utility, and society has not yet reached a consensus on how, whether, or when such a compromise is to be reached.

There are a variety of policy concerns which need to be addressed in an orderly way. These include the level of security which can be applied technologically to protect valuable information assets, the ease with which they can deployed without handicapping the users of the networks. How can confidential traffic be insulated from the open public systems and how much protection can customers expect for their own personal data transiting a network environment?

CRIMINALITY is still in its infancy with respect to computer networks, as the recent prosecutions discussed above indicate. Society has not yet reached a consensus on the nature of the crime or the sanctions to be applied.

COMPENSABILITY awards monetary damages in compensation for losses suffered at the hands of others. There is a large body of tort law which can be applied to inadvertent losses incurred from the misuse of information technology. There also exists current and vast experience with government-insured loans to backup failing savings and loan institutions which might be applicable to computer software houses.

Traditionally the communications carriers have enjoyed an insulation from liability for more than the cost of the transmission of missent, lost, or mangled messages. However, most carriers have historically been adjuncts of their national governments which enjoy a certain amount of sovereign immunity in any event. As the carriers become more privatized and more competitive, and the information transmitted becomes

more valuable in transit, major users are beginning to urge that the carriers undertake the recompense of more than the cost of information transfer.[121] The insurance industry has a major stake in the resolution of where the burdens should lie.

TRADEABILITY covers the rules under which information is marketed and sold as a commodity. The work going forward in the GATT toward evolving a code of ethical and legally enforceable conduct in the trade of information services is an important pioneering work.

PUBLICITY is a right to control the release of proprietary information at a time and place or one's choosing. This concept has been established by entertainment stars, such as Bette Midler, seeking to protect the commercial interest in their voices, personality, and style of acting.

COMPETENCY involves the need to qualify providers, users, or processors of information. Should computer users be tested and certified competent in order for them to have access to computer networks? Or would this infringe on First Amendment rights to freedom of speech? There is a long history of licensing requirements for drivers of automobiles and other dangerous behavior. There is a rich history of educational requirements and examinations to become a doctor or lawyer, a beautician, even a mechanic. However, the nature of the electronic environment is such that speech is very much involved. Moreover, there is much more than speech affected. Patients rely upon monitors which can mean the difference between life and death. Should network access be considered more like an exercise of free speech or entry into a critical profession?

CHAPTER ELEVEN

OBSERVATIONS

Clearly there exists a rich history of established legal concepts from which to draw experience but there remain many unanswered questions concerning their applicability to the rapidly changing environment of information assets. There are many forums in which issues concerning proprietary rights in information assets are currently being debated. These range from administrative agencies such as the copyright and patent offices, through numerous Congressional committees, many courts both domestic and foreign, corporate committees, international institutions, and transnational organizations. Therefore, a unified theory of information rights is far from being promulgated either nationally or globally.

Each forum contributes a different perspective. For example, the advantage of dealing with intellectual property rights in the GATT rather than WIPO is that one can trade off advantages in other sectors or hold hostage trade in other products in order to negotiate a more favorable environment. The reason that the United States has begun experimenting with such new legislation as the Section 301 provisions of the Trade Act is that traditional methods of dealing with the problem of piracy of information have not been successful.

Initiatives abound both in public and private forums. Thoughtful discussions are taking place all over the globe. A coherent policy will, no doubt, develop with all deliberate speed; but that speed may not be sufficient to keep ahead of new developments in technological capabilities.

There is a strong interplay between the technology, the marketplace, and the law. The history of cable television is particularly fraught with frustrated programmers whose product has been first pirated (at least arguably so) then permitted as a *fait accompli*.[122] In the Fortnightly case, the Supreme Court could have as easily held that cable television systems were retransmitting the broadcast signal to their

viewers, thus requiring them to pay compensation to the program producers. The trial court did so hold. However, by the time the case reached the Supreme Court, cable television was a marginal but healthy service permitting viewers at the fringes of broadcast contours to receive an improved signal of what was, in fact, a signal largely paid for by the advertisers. Thus the pragmatic decision favored delivery of what was then called CATV as merely an enhancement of a broadcast signal which the viewer was already entitled to receive.

By the time the legality of backyard satellite dishes reached the courts, there were enough residential owners relying upon the service that an exception to the prohibitions against interception of the signal had to be carved out by the Congress. These owners were permitted "private viewing" of signals that were not otherwise encrypted or marketed fairly to potential subscribers.

Similarly with the videocassette recorder, there were so many in use recording off the air, that a "private use" exception had to be carved out to save the practice from potential prosecution as a copyright violation. So it was with photocopying that the "fair use" doctrine absorbed duplications for personal use. Substantially the same kind of exception is being carved out for "private copying" of computer software in the European Community's current proposals.

So long as the technology facilitates the pirating, or unauthorized taking of program sources without compensation, the temptation will remain great. As always, the judiciary must consider what is considered to be ethical practice and what can reasonably be enforced by the legal system. There is an old saying that possession is nine-tenths of the law. Many consumers, with the technology aiding and abetting, are acting upon this assumption. Moreover, the economic theorists, currently in vogue, encourage regulatory restraint, leaving the marketplace to determine the course of history. The law cannot, at least in a democracy, outpace the development of consensual ethical norms. As a consequence, a coherent legal regime, appropriate to the

global trend in privatization of information resources, may be long in coming.

What remains for the future is a careful reconsideration of the value of information assets as a commodity on an open and competitive global marketplace. It may become necessary to redraw the lines between public and private dissemination of information resources to assure that the entrepreneurial efforts are adequately compensated to bring new product to market. As privatization of information resources and telecommunications transport accelerates, not only in the United States but worldwide, the necessity to rethink the dividing line between public and private custody of information becomes more critical. Many of the current practices belong to an era of substantial government subsidy of information dissemination which seems to be on the wane.

Some of the time-honored principles of intellectual property law need to be reviewed and rethought especially with respect to the treatment of computer software. What is predominantly a utilitarian product does not fit neatly into a system designed for artistic and literary works, even though the system can be stretched to accommodate the incorporation of software within its bounds. An intellectual asset so valuable needs to be treated as such. That which is utilitarian is in constant use. It would seem that its use is what requires compensation rather than its copies. In a world of interconnected computer-based access to central databases worldwide, there may be only one or a few "copies" of the information assets. However, the uses may be myriad and varied and widely dispersed.

Striking a balance of equities among the sources, the processors, and the users of such intellectual assets is the challenge which confronts lawyers and legislators, as well as the designers, producers, and custodians of information products. Such efforts will proceed apace in the marketplace, whether by contract, by chance, or by choice; within legislative bodies, whether by design or by default; within judicial bodies whether governed by wisdom or by folly; and through mediation as well as arbitration and accommodation. Pioneering efforts to draft

viable and enforceable laws governing information assets are destined to find a rich and diverse future as the "information age" reaches maturity.

NOTES

1. U.S. v. Robert Tappan Morris, Northern District of New York, No. 89-CR-139, May 4, 1990, 2 CCH Computer Cases ¶46,301 at 62,208.

2. 985 F.2d 504 (2d Cir. 1991), 2 CCH Computer Cases ¶46,419.

3. The U.S. Attorney for the Northern District of New York commented: "It was extremely difficult in this case to strike a fair balance between the unique circumstances surrounding Robert Morris' conduct and the goal of deterring future computer-related crime. Judge Munson's efforts to fashion an equitable sentence in this particular case will not weaken the resolve on the part of Federal authorities to prosecute computer offenses vigorously. Among other things, the Morris case should put the would-be hacker on notice that the Department of Justice will seek severe penalties against future computer criminals, whether or not they are motivated by a venal or malicious intent." 2 CCH Computer Cases ¶46,301 at 62,209.

4. Three young members of a computer group called "Legion of Doom" (whose computer aliases were "The Leftist," "Necron 99," and "The Prophet") entered guilty pleas and were sentenced in Atlanta for unauthorized access to and possession of 15 BellSouth access devices with the intent to use them to defraud. Two of the three were given 14-month prison terms and the third, with a prior computer fraud conviction, 21 months. They were also ordered to pay restitution of $233,000. A spokesman for BellSouth stated that the three had caused the company to spend $1.5 million in pursuing the miscreants and another $3 million to improve network security.

5. A/Conf.144/L.11, 4 September 1990, Agenda item 3.

6. Northern District of Illinois, Eastern Division No. 90 CR0070, July 3, 1990, 2 CCH Computer Cases ¶46,316. "It is well settled that when proprietary business information is affixed to some tangible medium, such as a piece of paper, it constitutes 'goods, wares, or merchandise' within the meaning of Section 2314.... This court sees no reason to hold differently simply because Neidorf stored the information inside computers instead of printing it out on paper."

7. 925 F. 2d 130 1301 (10th Cir. 1991), 2 CCH Computer Cases ¶46,415 at 62,901: "We hold that the computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods, wares merchandise, securities or moneys which have been stolen, converted or taken within the meaning of Sections 2314 or 2315."

8. Henley Holdings, Inc. v. Dept. of Revenue, State of Florida, 3 CCH Computer Cases ¶46,523 at 63,453. (2d Judicial Circuit, Florida, Leon County, No. 4381, July 22, 1991). "The word 'tangible' derives from the Latin word 'tangere,' meaning 'to touch'.... Even if Bunker Ramo's business could properly be characterized as the sale of 'images,' those

screen displays are not capable of being touched, subject to manual possession or movable."

9. U.S. General Accounting Office, Report to the Chairman, Subcommittee on Courts, Intellectual Property and the Administration of Justice, Committee on the Judiciary, House of Representatives, *Technology Transfer: Copyright Law Constrains Commercialization of Some Federal Software*, GAO/RCED-90-145, June 1, 1990.

10. H.R. 191 introduced January 3, 1991, would amend the Stevenson-Wydler Technology Innovation Act of 1980 to facilitate technology transfer through transferring copyright proprietorship for works prepared under cooperative research and development agreements (CRADAS). Royalties would also be payable to government employees who created the software in much the same manner that royalties are permitted to be paid to government inventors under the Federal Technology Transfer Act of 1986.

11. 49 *Guide to Computer Law* 5, CCH, 1991.

12. The Computer Software Rental Amendments Act of 1990 (Title VIII), along with the Visual Artists Rights Act of 1990 (Title VI) and the Architectural Works Copyright Protection Act (Title VII), was incorporated into the Civil Justice Reform Act (P.L. 101-650) and signed into law by President Bush on December 1, 1990. The legislation created a very narrow exception to the "first sale" doctrine of the Copyright Act, requiring the copyright holder's permission for the rental, loan, or lease of copyrighted software for direct or indirect commercial gain but excluding from this requirement lending by nonprofit libraries, leasing of software incorporated into computer equipment, and rental of computer games.

13. Article 4.

14. For a discussion of emerging issues, see Jack Shandle, "Multimedia Computing Hits a Sour Note," *Electronics* (June 1991), 48-53.

15. Article 1 (1).

16. Article 5 (3).

17. Article 41.

18. Article 6 (1).

19. Article 6 (2) (c).

20. Feist Publications, Inc. v. Rural Telephone Co., Inc. 2 CCH Computer Cases ¶46,423–U.S. (1991), reversing 916 F. 2d 718 (10th Cir. 1989).

21. For example, a company assigned an 800 number by one carrier may wish to transfer that number when it decides to change carriers, but the carrier that assigned it may claim a proprietary interest in the number

and refuse to permit the company to port the number along with its patronage.

22. "Rural may have been the first to discover and report the names, towns, and telephone numbers of its subscribers, but this data does not '"ow[e] its origin"' to Rural.... Rather, these bits of information are uncopyrightable facts." 2 CCH Computer Cases ¶46,423 at 62,957.

23. To quote Justice O'Connor: "Originality is a constitutional requirement. The source of Congress' power to enact copyright laws is Article I, Section 8, clause 8, of the Constitution, which authorizes Congress to 'secur[e] for limited Times to Authors ... the exclusive Right to their respective Writings.' In two decisions from the late 19th Century – The Trade-Mark Cases, 100 U.S. 82 (1879); and Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (18874) – this Court defined the crucial terms 'authors' and 'writings.' In so doing, the Court made it unmistakably clear that these terms presuppose a degree of originality." 2 CCH Computer Cases ¶46,423 at 62,952.

24. 2 CCH Computer Cases ¶46,423 at 62,958.

25. Mark S. Nadel, "Rings of Privacy: Unsolicited Telephone Calls and the Right of Privacy," 4 Yale J. on Reg. 99 (1986).

26. For a discussion of this and similar issues, see Anne W. Branscomb, "Common Law for the Electronic Frontier," *Scientific American* (September 1991), 154.

27. See Draft Proposals for Council Directives, *Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, Com (90) 314-C3-323/90 - SYN 287, and *Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks*, Com (90) 314-C3-323/90 - SYN 288.

28. For a good summary of the history and present state of privacy protection in the U.S., see, Ronald L. Plesser and Emilio W. Cividanes, *Privacy Protection in the United States: A 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector Including a List of All Relevant Officials* (Washington, D.C.: Piper & Marbury, 1991).

29. The author's extensive concern and involvement in these debates made it difficult to deal succinctly with a subject all too familiar in considerable detail. See "Computers and Intellectual Property," Hearings Before the Subcommittee on Courts, Intellectual Property, and the Administration of Justice, Committee on the Judiciary, House of Representatives, 101st Cong., November 8, 1989 and March 7, 1990, Serial 119.

30. Several cases are making their way up through the courts at the present time. These include Apple Computer v. Microsoft Corp. and Hewlett Packard, Civil Case No. C-88-20149 (VRW) (N.D. Cal.), and Lotus

Development Corp. v. Borland, Civil Action No. 90-11662-K (U.S.D.C. Mass.), which is to be decided by the same judge who decided Lotus Development Corp. v. Paperback Software International, 740 F. Supp. 37 (D. Mass. 1990). The latter case upheld a copyright in the Lotus' interface in its popular 1-2-3 spreadsheet program. Professor Samuelson criticizes the Paperback decision, in a paper to be published in 1992 in *Law and Contemporary Problems*, on the basis that it ignores that Section 102 (b) of the Copyright Act specifically inserted in the 1976 act to insure "that the actual processes or methods embodied in the program are not within the scope of copyright law." Section 102 (b) states: "In no event does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle or discovery."

31. "Fair Use" is a legal concept used to justify the copying of portions of works (and sometimes entire works) for purposes which have a public interest such as critical comment, education, or to archive for protection of source materials. "Reverse engineering" is a legal concept used originally in patent law to permit the taking apart of machinery in order to learn how it works better to enable the building of a better product, more recently employed as a rationale for decompilation of computer software in order to provide interoperability and compatibility of interfaces. The"first sale" rule prohibits a seller from controlling the use of a legally protected asset after it has been "sold." In order to avoid the consequences this has led to the development of elaborate "shrink wrap licenses" in the software industry which purport to render what appears to be a "sale" to the purchasers legally into a lease with certain prohibitions against copying, resale, etc. "Moral rights" are those which are retained by a creator of a work in order to maintain its integrity after it has been transferred to third parties. "Compulsory licensing" is a legal concept which permits a form of "taking" without the agreement of the creator or owner of information providing for statutory compensation rather than a negotiated price.

32. The Free Software Foundation, Inc., 675 Massachusetts Avenue, Cambridge, MA 02139, publishes a GNU bulletin semiannually in which it espouses a new concept of "copyleft" guaranteeing freedom of access to their software and prohibiting anyone from claiming a proprietary interest in any modification of it, thus encouraging the sharing. This is apparently a recognition that putting software into the public domain does not necessarily result in preventing others from using components to enhance their proprietary products. See also Richard Stallman, "Why Software Ownership is Bad for Society," speech at the University of Texas, 1987; "A Battle to Make Software Free," *New York Times* (Jan. 11, 1989) C1; "The Hacker's Return," *The Economist* (July 13, 1989), 81. Richard Stallman has also organized the League for Programming Freedom which is intended to protest the monopolization of common user interfaces through the "look and feel" litigation in the courts. Recently the League held a rally to picket the Lotus Development Corporation which has filed several such suits against its competitors who have incorporated compatible interfaces which are arguably proprietary to Lotus.

33. This incident was reported to have occurred in the CERN facilities near Geneva.

34. The Law Commission (Law Com. No. 186) "Criminal Law and Computer Misuse," Presented to Parliament by the Lord High Chancellor by Command of Her Majesty, October 1989.

35. Michael Specter, *The Boston Globe* (Dec. 15, 1989), 8.

36. Kristi Umbreit, "Man Held in Alleged Computer Extortion," *AP via LEXIS* (Feb. 3, 1990); Michael Alexander, "Suspect arrested in AIDS disk fraud case," *Computerworld* (Feb. 5, 1990) 8.

37. A review of several of the more widely publicized incidents is contained in either of two articles written by the author, Anne W. Branscomb, "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime," 16 *Rutgers Computer and Technology Law Journal* 1-61 (Winter 1990); "Rogue Computer Programs – Viruses, Worms, Trojan Horses, and Time Bombs: Prank, Prowess, Protection, or Prosecution?" (Cambridge, Mass.: Harvard Program on Information Resources Policy, September 1989).

38. The Cornell Report has a comprehensive appraisal of the incident: M. Stuart Lynn, Commission Chair, et al., *The Worm: A Report to the Provost of Cornell University and an Investigation Conducted by the Commission of Preliminary Inquiry*, Cornell University, Feb. 5, 1989, reprinted in *Communications of the ACM*, vol. 32, no. 6 (June 1908), 706.

39. The search for the hackers is documented by Clifford Stoll in *The Cuckoo's Egg* (Garden City, N.Y.: Doubleday, 1989).

40. Coy, Peter, "Computer 'Worm' Penetrates Scientific Computers," *AP via LEXIS*, Oct. 18, 1989.

41. Hearings on Computer Virus Legislation, November 8, 1989, before the Schumer Committee, Subcommittee on Criminal Justice of the Committee on Judiciary, U.S. House of Representatives.

42. Geoffrey Rowan, "Electronic Thieves are Tough to Thwart," *Globe and Mail Canada* (May 14, 1990), B1.

43. A meeting was recently held in Toronto, Canada, at the invitation of the Royal Bank of Canada to address such cooperation to protect the valuable information assets of financial institutions worldwide. According to James C. Grant, executive vice president of the Royal Bank, "Legal systems of different countries treat information differently, giving cause for concern to industry in general and to banking in particular." The meeting, which included representatives of banks, prosecuting attorneys, security experts, and government officials from three continents, discussed the need for pooling intelligence, cooperation across boundaries of law enforcement agencies, reform of the laws to empower agencies to cope with the new problems, and the need for heightened attention to training professionals to investigate and prosecute infractions of the laws. Reported "International Solutions to

Protect Financial Networks Needed," *Transnational Data and Communications Report* (April 1990), 7.

44. Harold L. Burstyn, "RTM and the Worm that Ate Internet," *Harvard Magazine* (May-June 1990), 23.

45. John Markoff, "Drive to Counter Computer Crime Aims at Invaders," *New York Times* (June 3, 1990), 1.

46. United States of America v. Robert Riggs and Craig Neidorf, No. 90 Cr 70, U.S. District Court for the Northern District of Illinois, filed July 6, 1990.

47. Ibid. The case was dismissed without prosecution.

48. "Cyberpunks are a 'counter-culture' who have allied themselves with Technology; in the service of a fast rich life," from J. A. Farrell, "The Cyberpunk Controversy," *The Boston Globe Magazine* (Feb. 19, 1989), 18.

49. Three members of the Legion of Doom pleaded guilty to conspiring to defraud BellSouth Corporation of computer information, unauthorized access to, and tampering with BellSouth's computer systems. *Wall Street Journal* (July 10, 1990), B4.

50. Ibid.

51. The proposed Computer Misuse Bill received its second reading in Parliament in February of 1990 and began its committee stage in the House of Commons on March 12, 1990.

52. The Computer Abuse Amendments Act of 1990, S. 2476, was introduced into the U.S. Senate by Senator Leahy on April 19, 1990, and hearings were held on July 31, 1990, by the Subcommittee on Technology and Law Committee of the Committee on the Judiciary.

53. Eli M. Noam, "Second Discussion Draft for a Notice of Inquiry on Privacy in Telecommunications Services," State of New York Public Utilities Commission, November 29, 1989.

54. For a full review of current and proposed state legislation in the United States, see Anne W. Branscomb, "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime," 16 *Rutgers Computer and Technology Law Journal* (Winter 1990), 1-61.

55. There were no restrictions on works emanating from government sources prior to 1895 when the Government Printing Office was established by the Printing Act of 1895 which included a prohibition against copyright of government sources documents. This was intended to prohibit private sector publishers, to whom duplicate printing plates could be sold, from claiming a proprietary interest and royalties from the republication thereof.

56. 17 U.S.C. Sec. 105 provides "Copyright Protection under this title is not available for any work of the United States Government, but the United States Government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise." There are only two exceptions, one for standard reference data, 17 U.S.C.Sec.290(e), P. L. 90-396, 82 Stat. 339 (1968) and the other for postage stamp designs, H.R. Rep. No. 94-1476, 94th Cong. 2d Sess. (1976).

57. Stevenson-Wydler Technology Innovation Act, P.L., 96-480; 15 U.S.C. Sec. 3710 (1988).

58. Report of the Register of Copyrights on the General Revision of the U.S. Copyright Law, 87th Cong. 1st Sess. 133 (House Committee Print 1961).

59. Supplementary Report of the Register of Copyrights on the General Revision of the U.S. Copyright Law, 89th Cong., 1st Sess. 10 (Committee Print 1965).

60. This clause in the Copyright Act was targeted by the author as a prime area for reform in testimony before the Kastenmeier Committee in an oversight hearing on November 8, 1990. See Testimony of Anne W. Branscomb, "Protecting the Crown Jewels of the Information Economy – The Legal Protection of Computer Software as an Intellectual Asset: An Overview of Policy Issues for Congressional Oversight," Testimony before the Subcommittee on Courts Intellectual Property, and Administration of Justice, U.S. House of Representatives, November 8, 1989.

61. Testimony of Ralph Oman Before the Subcommittee on Science, Research, and Technology, Committee on Science, Space, and Technology, House of Representatives, 101st Cong. 2d Sess., April 26, 1990.

62. Testimony of Bruce M. Winchell, General Patent Counsel, Martin Marietta Energy Systems, Inc., Oak Ridge, Tennessee, Before the Committee on Science, Space, and Technology, "Hearing on Copyright Protection for Intellectual Property to Enhance Technology Transfer," April 26, 1990.

63. Statement by Dr. Beatrice J. Farr, Senior Research Psychologist, Department of the Army, Before the House Committee on Science, Space, and Technology on Copyright Protection for Intellectual Property to Enhance Technology Transfer," April 26, 1990.

64. Kyoto News Service via LEXIS, May 15, 1990.

65. Anne W. Branscomb, "Protecting the Crown Jewels of the Information Economy," Chapter 4, in *Intellectual Property Rights in Science, Technology, and Economic Performance*, ed. Francis W. Rushing and Carole Ganz Brown (Boulder, Colo.: Westview Press, 1990), 47.

66. American Arbitration Association, Commercial Arbitration Tribunal, Case No. 13T-117-0636-85, International Business Machines Corporation v. Fujitsu Ltd., decided November 29, 1988.

67. Fortnightly Corp. v. United Artists Television, 392 U.S. 390, 88 S. Ct. 2084 (1968), rehearing denied, 393 U.S 902, 89 S. Ct. 65.

68. 47 C.F.R. Sec 76.61 (b) (2).

69. Rules re Microwave-Served CATV, First Report and Order, 38 FCC 683, 4 R.R.1725 (1965); Cable Television, Second Report and Order, 2 FCC2d 725, 6 R.R.1717 (1966), *aff'd, Black Hills Video Corp. v. FCC*, 399 F. 2d 65 (8th Cir. 1968).

70. Quincy Cable TV, Inc., 768 F.2d 1434, 1454 (D.C. Cir. 1985) cert. denied, 106 S. Ct. 2889 (1986).

71. 47 U.S.C.A. Sec. 605, 48 Stat. 1103 (1934), until it was amended, prohibited the unauthorized interception of radio and wire communications only, leaving the question of satellite and data interception unclarified. Section 634 of the Cable Communications Act of 1984, 47 U.S.C.A. Sec 634, prohibited the unauthorized interception of services offered "over a cable system."

72. P.L. 98-549, 98 Stat. 2779.

73. Reregulation of Receive-Only Domestic Earth Stations, 74 F.C.C., 2d 205, 216, 46 R.R. 2d 511 (1979).

74. 47 U.S.C.A. 605 (b). For the reasoning behind this exception of Section 605 for the earth station community, see 130 Cong. Rec. H. 10439, H10443 (Oct. 1, 1984), remarks of Senators Gore and Wirth, and 130 Cong. Rec. S14287 (Oct. 11, 1984), remarks of Senator Packwood, the latter reprinted in 1984 U.S. Code Cong. & Ad. News 4746.

75. Satellite Home Viewers Act of 1988. P.L. 100-667, S. 1883.

76. Sony Corporation America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

77. For a very interesting article on the applicability of the doctrine to computer software, see David Rice, "Licensing the Use of Computer Program Copies and the Copyright Act First Sale Doctrine." 30 *Jurimetrics Journal* 157 (Winter 1990).

78. Legislation has been introduced in both houses of Congress, in the House by Representative Synar, H.R. 2740; the Senate passed S. 198, the bill introduced by Senator Hatch, by voice vote on May 1, 1990.

79. "Mr. Smith, and Friend Jimmy Stewart, Movie Colorization," *Broadcasting Magazine*, vol. 114 (Mar. 21, 1988), 49.

80. What Congress devised was a National Film Preservation Board with authorization to designate 25 films each year as classics which could be advertised in their original form as such. See David Goeller, "House Would Discourage but not Ban Colorized Movies," *AP via LEXIS*, June 30, 1988. The legislation establishing a National Film Preservation Board is to be found in Title 2, Chapter 5, 2 USCS Sec. 178j (1989).

81. "Copyright Registration for Colorized Versions of Black and White Motion Pictures," Docket No. RM 86-1A, 52 Fed. Reg. 23443, June 22, 1987.

82. An article entitled "Photography's New Bag of Tricks" in the *New York Times Magazine* (Nov. 4, 1984) reported this incident and further claimed that "In ten years we will be able to bring Clark Gable back and put him in a new show."

83. Bette Midler v. Ford Motor Co., 849 F. 2d 1988 (9th Cir. 1988), LEXIS 8424, reversing Bette Midler v. Ford Motor Co., LEXIS 14367 (C.D. CA 1987).

84. For an interesting discussion of the issues, see Andy Grundberg, "Ask It No Questions: The Camera Can Lie," *New York Times*, Section 2 "Arts & Leisure" (Aug. 12, 1990), 1.

85. Mead Data Central v. West Publishing Co., Case No. C-3-87-426 (U.S. District Court, S. D. Ohio). Katherine M. Hafner, "Whose Page Numbers Are They, Anyway?" *Business Week* (Aug. 8, 1988), 70E.

86. Proposal for a Council Directive on Legal Protection of Computer Programs, Submitted by the Commission on 5 January 1989 Com (88) 816 Final - Syn 183,89/C91/05. For a short summary of arguments for and against, see Mark Turner, "Generality mars EC software draft," *Financial Times* (May 31, 1990), 12.

87. A very exhaustive exploration of the alternatives is to be found in Duncan Davidson, Chairman, "Protecting Computer Software: A Comprehensive Analysis," *Arizona State Law Journal* 611 (1983), Report of the Computer Law Division of the American Bar Association Science and Technology Section.

88. A better term may be "reverse analysis."

89. See the statement of Michael Jacobs representing Fujitsu at the LaST Frontier Conference on Software at the Arizona State University Conference on Computer Software, February 13, 1989.

90. Comments of the Computer and Business Equipment Manufacturers Association (CBEMA) to the U.S. Trade Representative Concerning a Proposal for a Directive by the Council of the European Economic Community on the Legal Protection of Computer Programs, January 22, 1990.

91. Letter to Mosbacher, March 1, 1990, signed by a dozen Congressmen including Markey, Gibbons, Guorini, Walgren, and Synar, Ritter, Campbell, and Neel. Other signatures are undecipherable.

92. Alan Westin has thoughtfully defined privacy as "the claim of individuals, groups, or institutions to determine themselves when, how, and to what extent information about them is communicated to others." *Privacy and Freedom* (New York, N.Y.: Atheneum, 1970), 7. Since this definition could equally be applied to publicity, perhaps it is more

useful to define privacy as the ability to prevent disclosure or intrusion, whereas publicity is the right to control the distribution of information.

93. Mary Lu Carnavale and Julie Amparano Lopez, "Party Line, Making a Phone Call Might Mean Telling the World About You," *The Wall Street Journal* (Nov. 28, 1989), 1.

94. For an overview of legal issues related to ANI, see Glenn Chamas Smith, "Caller Identification Technology and the Right to Informational Privacy," 37 *UCLA L. Rev.* 145 (1989).

95. See Carnavale, *supra*, note 93.

96. "Caller ID Debate," *Transnational Data and Communications Report* (May 1990), 21.

97. Although the PUC authorized Bell Telephone of Company of Pennsylvania to offer Caller ID services in December 1989, a stay was obtained in the Pennsylvania Commonwealth Court. David M. Barasch v. Pennsylvania Public Utility Commission, No. 2270 C.D. 1989, filed May 30, 1990. The PUC will require some limited blocking capability, and a bill has been introduced into the legislature to require that customers be able to block transmission of their telephone number on an individual basis.

98. TR International (July 6, 1990) 6.

99. David Nyhan, "Judges Dial Wrong Number This Time," *The Boston Globe* (June 3, 1990), A25; Lawrence Edelman, "Is This Man Invading Your Privacy?" *The Boston Globe* (November 20, 1990), 25.

100. Equifax Survey conducted by Louis Harris & Associates, 1990.

101. Ibid., p. xxiii.

102. P.L. 98-549;98 Stat. 2779; 47 U.S.C. Sec. 551.

103. The Video Privacy Protection Act of 1988, P.L.100-618, 102 stat. 3195, 18 U.S.C. of 2710. The legislation is popularly referred to as the Bork Bill. "Protect Our Rights to Privacy and Secrecy," *USA Today* (April 12, 1989), 10A.

104. For a review of the present situation with respect to transaction generated information of which corporations are the custodian, see Thomas E. McManus, "Telephone Transaction-Generated Information: Rights and Restrictions" (Cambridge, Mass.: Harvard University Program on Information Resources Policy, May 1990).

105. "My other car is a . . . ," *The Economist* (Feb. 10, 1990), 64.

106. "Mail-order companies," *Consumer Reports* (Oct. 1987), 607.

107. Melinda Grenier Guiles, "Why Melinda S. Gets Ads for Panty Hose, Melinda F., Porsches," *Wall Street Journal* (May 5, 1988), 1.

108. See *Consumer Reports* article, *supra*, note 106.

109. Council of Europe Guidelines, "Protection of Personal Data for the Purposes of Direct Marketing" (ISBN 92-871-0876-5), reported in *Privacy Journal*, vol. XIII, no. 4 (February 1987).

110. Rowan v. United States, 397 U.S. 728 (1970).

111. Equifax Survey, p. xxviii, Louis Harris & Associates, 1990.

112. "Privacy Study Reveals Lack of Consumer Confidence," *Direct Marketing* (December 1988), 8.

113. Kathryn Marchocki, "Prize letters, phone spiels top list of consumer beefs," *The Boston Herald* (Jan. 5, 1989), 47.

114. This is a legal discipline taught regularly in many law schools today.

115. According to Jeff Johnson, writing in the newsletter of the Computer Professionals for Social Responsibility, the question is, "Which privacy right is more important: the right to prevent your telephone number from being disclosed to others, or the right to know who is calling you?" "Caller Identification: More Privacy or Less?" *The CPSR Newsletter* (Winter-Spring 1990), 1-6.

116. "Some believed that Mr. Newman's writings, stored on a computer disk, were the property of the community and not his to destroy," John Markoff, "Programmed for Life and Death," *New York Times*, Section 4 "The Week in Review" (Aug. 26, 1990), 4, c. 1.

117. Stuart J. Johnston, "Computer Virus Spreads to Commercial Software," *Infoworld* (Mar. 21, 1988), 85.

118. 47 C.F.R. Sections 73.123; 73.300;73.598; 73.679.

119. Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241 (1974).

120. See Nolan Bowie, "Equity and Access to Information Techonology," *The Annual Review*, Institute for Information Studies (1990), 131-177.

121. James Grant, Vice President of the Royal Bank of Canada, has urged this concept in major telecommunications forums such as the International Telecommunications Union for a number of years already.

122. Ted Turner made the off-hand comment at a conference, organized recently by the Federal Communications Bar Association, that cable systems no longer had to steal their product from broadcasters. Turner Broadcasting is a good example of successful innovation in the cable television industry, offering the first "super station" delivering an intended original program for cable systems from its Channel 17 UHF

station in Atlanta, then offering the first all-news program received globally, CNN, starting a full-service programming service, TNT, and producing much original programming for first showing on cable television systems.