Volume 5, Spring Issue, 1992

NEW LAWS FOR NEW TECHNOLOGIES: CURRENT ISSUES FACING THE SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

Senator Patrick J. Leahy *

INTRODUCTION

The headlong pace of technological change in our society has become so familiar that we often take it for granted. With personal computers on every office desk and in millions of homes, we barely recall that the PC revolution is little more than a decade old. Personal computers themselves now often seem cumbersome as we watch laptops, notebooks, and soon, hand-held computers spread across the land.

The communications revolution is in full swing. We read now about a day when fiber optic "superhighways" will put enormous multimedia resources — voice, text, and video — at the fingertips of anyone with a home computer — and we know this is not the stuff of science fiction. We look forward to the dissemination of high-definition television, virtual reality, and artificial intelligence. These and other "back-to-the-future" wonders will continue to transform our world in the years and decades ahead. They will also create new challenges for our law and public policy.

In January 1987, the Subcommittee on Technology and the Law was established to study new technologies and to make sure that American law keeps pace with them and is responsive to their special characteristics. There are other committees in Congress, such as the Senate Commerce Committee's Science, Technology and Space Subcommittee, that focus explicitly on science and technology policy, examining, for example, what role the federal government should play in encouraging technological development. The mission of the Subcommittee on Technology and the Law, which I chair, is different. We turn our attention to the legal problems created by new technologies and the special legal responses that these technologies may require.

The Subcommittee on Technology and the Law is a reflection of Congress' desire to stay ahead of the curve. We need to analyze hi-tech

---

* United States Senator (D-Vermont). Chairman, Subcommittee on Technology and the Law of the Senate Committee on the Judiciary. The author wishes to thank Todd Stern, Catherine Russell, and Tris Coffin of his Technology and Law Subcommittee staff for their help in preparing this Article.

issues carefully, but in a timely fashion, so that the law reflects the realities of the marketplace. At present, there are a number of important issues on the Subcommittee's agenda. They raise questions concerning open government, our citizens' fundamental right to privacy, and the competitiveness of U.S. high technology.

I. COMPUTER SOFTWARE: DECOMPILATION

The creation of computer software was precisely the kind of issue that compels the attention of my Subcommittee. Here was a technology with characteristics unlike any other—partly expressive, partly functional. The initial question—raised long before the founding of the Technology Subcommittee—was how the law should protect this technology.

The Copyright Office first began accepting computer programs for copyright registration in 1964 under its so-called "rule of doubt,"[1] which signaled the office's uncertainty about how such programs should be protected. It did not become clear that computer programs would be protected by copyright until after the 1978 report of the National Commission on New Technological Uses of Copyrighted Works ("CONTU"),[2] which Congress had established four years earlier.[3] In 1980, following CONTU's recommendation, Congress passed the Computer Software Copyright Act, which established that computer programs were protected by copyright as literary works.[4]

The 1980 law laid the foundation for the legal protection of software, but, of necessity, left open many questions that have been and continue to be worked out in the courts. These questions include whether given aspects of computer programs are protectible expression or are unprotectible ideas and whether infringement may result from copying not just actual computer code, but the "structure, sequence, and organization" of

1. U.S. DEP'T OF COMMERCE, MANUAL OF PAT. EXAMINING PROC. §§ 2240, 2244 (5th ed., rev. 1989).

2. NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT (1978).

3. Pub. L. No. 93–573, 88 Stat. 1873 (1974) (codified at 17 U.S.C. § 701 (1988)).

4. Pub. L. No. 96–517, §§ 10(a)-(b), 94 Stat. 3015, 3028–29 (1980) (codified at 17 U.S.C. §§ 101, 117 (1988)).

a program[5] or the "look and feel"[6] of its user interface.

The issue that has come to demand congressional attention of late is decompilation, a form of reverse engineering. Software is written in code by computer programmers in one of several computer languages such as COBOL, FORTRAN, BASIC, or C. This code—and there may be hundreds of thousands of lines of code for a single program—is the "source code." For the computer to be able to execute it, the source code must be translated or "compiled" into machine-readable, binary language—the 0's and 1's that computers understand. This "object code" is commercially available to anyone with a copy of the program, while the underlying source code is typically unpublished and undisclosed.

Decompilation is the process by which a competitor or a researcher can disassemble or "decompile" a program's object code through use of a special decompiling program and reconstruct the human-readable source code. As an intermediate step in this process, it is necessary to make a copy of the original program. Unless justified by an exception in the Copyright Act, such as the fair use exception,[7] this copying would constitute copyright infringement.

Once the source code has been reconstructed—a process that can take considerable human effort over and above the work done by the decompiling program—a product can be created that is competitive with, but not a literal copy of, the original.

The necessity of decompilation and the extent to which it should be permitted are the sources of a debate that is currently raging not only in the United States, but also in international fora, such as the European Community and the World Intellectual Property Organization. The proponents of decompilation say that it is necessary for a number of rea-

---

5. *See, e.g.*, Whelan Assocs., Inc. v. Jaslow Dental Lab., Inc., 797 F.2d 1222 (3rd Cir. 1986), *cert. denied*, 479 U.S. 1301 (1987) (finding infringement, despite lack of literal copying, because of similarity in structure between the two programs); SAS Inst., Inc. v. S & H Computer Sys., Inc., 605 F. Supp. 816 (M.D. Tenn. 1985) (finding infringement because defendant's program followed organizational structure of plaintiff's program down to a detailed level).

6. *See, e.g.*, Johnson Controls, Inc. v. Phoenix Control Sys., Inc., 886 F.2d 1173 (9th Cir. 1989) (holding that a reasonable person in the intended audience would conclude that the infringing work captured the "total concept and feel" of the protected program). *But see* Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37, 68 (D. Mass. 1990) (after noting that the "look and feel" concept was not helpful in distinguishing between copyrightable and uncopyrightable elements of a computer program, court found that the "Lotus 1–2–3" spreadsheet was copyrightable because of the "menu structure, taken as a whole . . . including the choice of command terms, the structure and order of those terms, their presentation on the screen, and the long prompts," and that defendant was liable for infringement). *Id.*

7. 17 U.S.C. § 107 (1988).

sons. The first involves interfaces. In any computer system, there are a variety of points of attachment between software and hardware or between different kinds of software. For example, microcode creates the instruction set for a microprocessing chip that may serve as the brain of a personal computer. The microcode, embedded in the chip, is the software link between the hard-wired circuitry and the operating software (operating system) that governs the internal operations of the computer. Similarly, there are interfaces between an operating system and an applications program (such as a word processing program, a spreadsheet, or a game) that permit the operating system and applications program to work together or to "interoperate."

Unless the relevant interfaces are understood, the competitor cannot make a competing operating system that will interoperate with both hardware and the applications programs in the manner of the original operating system. Nor can a competitor make a competing applications program that will, for instance, run on the MS/DOS operating system unless it understands the interfaces necessary to make the new applications program compatible with MS/DOS.

Some proponents of decompilation go further and say that it is perfectly legitimate to use this technique, not just to discover the interfaces necessary to connect independently created programs, but to make competitive clones. They argue that clones, which provide new and improved features at lower cost, are good for consumers.

Opponents of decompilation contend that it allows the copier to take an unconscionable free ride on what may have been an enormous research and development effort to create the original program. They argue that the point of intellectual property protection is to provide an economic incentive so that creators will create. They say that if decompilation is given free rein this incentive will be diminished. The time lag between original creation and a clone made via decompilation is, they argue, too short to allow the creator to recoup its investment in research and development. They also fear that even if latitude were given to decompilation for the sole purpose of creating interfaces, that latitude would be abused and competitors would, in practice, still use the technique to create competitive products.

The issue has come to our attention in Congress in the context both of legislation and of international agreements. The legislation that presents this issue did so inadvertently. In 1987 and 1989, two decisions of the U.S. Court of Appeals for the Second Circuit—*Salinger v. Random House, Inc.*,[8] involving the unpublished letters of J.D. Salinger, and *New*

8. 811 F.2d 90 (2d Cir.), *cert. denied*, 484 U.S. 890 (1987).

Era Publications International v. Henry Holt & Co.,[9] involving the unpublished diaries and journals of Scientology founder L. Ron Hubbard—appeared to limit the doctrine of fair use as it applied to unpublished works. Dicta in those cases suggested that the absence of publication would be all but dispositive against an asserted claim of fair use.[10]

These cases sent shock waves through the publishing and writing community. Writers and historians asserted that they could not do their work if they had to seek permission for every unpublished letter or diary that they wished to quote and that, if forbidden to quote, their work product would lack the color and panache of good writing.

Senator Paul Simon and I introduced legislation in the 101st Congress[11] and again last year in the 102d Congress[12] to eliminate the per se implication of the *Salinger* and *New Era* cases with respect to unpublished materials and to restore the law of fair use to its position after the Supreme Court's 1985 ruling in *Harper & Row Publishers, Inc. v. Nation Enterprises*.[13]

As noted above, however, computer source code is unpublished. Much of the U.S. computer industry feared correctly that if, in rolling back the dicta of the *Salinger* and *New Era* cases, we went too far and gave a green light to the use of unpublished material, the legislation might be interpreted to condone the decompilation of computer programs. After lengthy negotiations with the publishing and computer industries, we worked out a consensus bill that passed the Senate in September 1991.[14] At this writing, we are looking forward to action from the House.[15]

Software copyright questions have also figured prominently on the international front. To appreciate the importance of tough intellectual property protection for software, a few facts must be noted. Software is a fifty-billion-dollar industry and is the most rapidly growing part of the computer business. Some estimate that it will be a *trillion*-dollar business by the end of this decade. Right now, the United States is the undisputed world leader, controlling some seventy percent of the market. The Japanese, meanwhile, have targeted software as an economic prior-

9. 873 F.2d 576 (2d Cir.), *reh'g denied*, 884 F. 2d 659 (2d Cir. 1989), *cert. denied*, 110 S. Ct. 1168 (1990).

10. *See* 811 F.2d at 95; 873 F.2d at 583–84.

11. S. 2370, 101st Cong., 2d Sess. (1990).

12. S. 1035, 102d Cong., 1st Sess. (1991).

13. 471 U.S. 539 (1985).

14. *See* 137 CONG. REC. S12,663 (daily ed. Sept. 10, 1991); *id.* at S13,923 (daily ed. Sept. 27, 1991).

15. *See* 137 CONG. REC. H7087 (daily ed. Sept. 30, 1991).

ity. Now, it is by no means fair to characterize the decompilation debate as simply a battle between American "creators" and Japanese "copiers" seeking the shortest route to increased market share; after all, many American companies also favor decompilation. But it is nonetheless true that Japanese companies are among the most vocal proponents of decompilation.

In the Uruguay Round negotiations of the GATT, lengthy talks have been necessary to establish that computer programs are to be protected as literary works under the Berne Copyright Convention, the world's leading copyright treaty.[16] In May 1991, I chaired Part II of a two-part hearing in the Patents, Copyrights and Trademarks Subcommittee to consider the intellectual property negotiations in the Uruguay Round.[17] I directed particular attention to computer programs and the need for a regime of tough international protection.

Last November, the World Intellectual Property Organization, a United Nations body that administers the Berne Convention, initiated a multi-year consideration of whether a new protocol should be added to the Convention, covering, among other things, computer programs and decompilation. Whether a new protocol will be produced and, if so, what it will say, are far from clear at this point.

Meanwhile, the European Community, as part of its ongoing effort to construct a single market, has been attempting to harmonize the commercial laws of its member states. In December 1990, the EC issued its directive on the protection of computer programs, which includes a much debated section on decompilation. In essence, the Directive permits decompilation when it is indispensable to achieve interoperability of an independently created computer program with other programs, but not for the purpose of making and marketing competitive products.[18]

II. NATIONAL INFORMATION NETWORK

Bit by bit this nation is approaching the day when our people and our businesses will be linked together in a vast electronic network over which voice, data, text, and video will flow seamlessly.

More and more information is linked by new computer and telephone

16. The Berne Convention for the Protection of Literary and Artistic Works, 828 U.N.T.S. 221 (opened for signature Sept. 9, 1886); *see* The Berne Convention Implementation Act of 1988, Pub. L. No. 100–568, 102 Stat. 2853 (1988).

17. Senator Dennis DeConcini (D-Ariz.) is Chairman of the Patents, Copyrights and Trademarks Subcommittee.

18. Council Directive on the Legal Protection of Computer Programs, Dec. 14, 1990, at 11–12.

systems. Today, Internet, the largest computer network in the country, links hundreds of private, State, and federal research networks, including the National Science Foundation's network ("NSFNET"), which connects more than 500 colleges and universities. The resulting free flow of information enhances academic research and contributes significantly to American competitiveness abroad.[19]

In an effort to expand the nation's capacity to communicate on computer networks, Congress passed legislation last year directing the National Science Foundation, the Departments of Defense and Energy, and NASA to work together toward the deployment of a National Research and Education Network ("NREN")[20] by 1996. The NREN will be capable of transmitting extraordinary amounts of information to and from supercomputers at lightning speed. The high-performance computer technology that makes this communication possible is comprised of "the most sophisticated computer chips, the fastest computers with the largest memories, the fastest algorithms, and the fastest networks."[21] The NREN will not only connect huge computer centers; it will also make it possible for individuals all over the country to communicate with each other by electronic mail.[22]

Computers are only one piece of the communications structure of the future. The telephone industry is moving rapidly toward fully digitized systems that will permit simultaneous voice and data communication over the same phone line. Video—like cable or motion pictures—will also travel over telephone lines.

In addition, as the result of recent court decisions, the seven regional Bell Operating Companies ("BOCs")—which had been barred from the business of offering information services under the terms of the consent decree that broke up AT&T[23]—are starting to offer such services on their own, rather than just providing the common carriage wires over which other companies provide services such as LEXIS, Prodigy, and Dow Jones.[24]

---

19. *See generally Information and Competitiveness: Hearing Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary*, 100th Cong., 1st Sess. (1988).

20. *See* The High-Performance Computing and National Research and Educational Network Act of 1991, Pub. L. No. 102–194, 105 Stat. 1594 (1991).

21. S. REP. NO. 57, 102d Cong., 1st Sess. 1 (1991).

22. *Id.* at 3.

23. United States v. American Tel. & Tel. Co., 552 F. Supp. 131 (D.D.C. 1982), *aff'd sub nom.*, Maryland v. United States, 460 U.S. 1001 (1983).

24. The BOCs were created as part of the 1984 modified final judgment ("MFJ") settling the Justice Department's decade-old antitrust suit against AT&T. *See id.* Under the terms of the MFJ, AT&T divested itself of its 22 wholly owned operating companies, and the seven BOCs were created. AT&T was left with a long-distance and manufacturing business and the freedom to enter other fields. The BOCs were left to provide local phone service and were barred from entering three lines of business—manufacturing, long distance,

Legislation now pending in Congress, sponsored by Senator Inouye (D-Hawaii)[25] and Representative Cooper (D-Tennessee),[26] would once again bar the BOCs from the information services business until there is genuine competition in their local exchange areas. Representative Jack Brooks (D-Texas), Chairman of the House Judiciary Committee, is also considering legislation that would restrict the BOCs' ability to offer information services. The newspaper industry and many companies that deliver information services over the phone wires vehemently oppose entry by the BOCs into the information industry and support this legislation. It is possible that some restrictions will be placed on the BOCs, but it is doubtful that the phone companies will be prevented for very long from offering information services.

What all of this means is that a national public network infrastructure will develop during this decade and the next. It will, in the words of Mitch Kapor, former CEO of Lotus, "emerge from the 'convergence' of the public telephone network, the cable television distribution system, and other networks such as the Internet."[27]

The prospect of an electronic network tying our national community together interactively is fascinating and exciting. Technology will open channels of communication in education, business, and entertainment from the country's largest cities to its most remote areas. But the development of this network also raises a host of legal and policy questions.

First, how can we best ensure easy access to the network for informa-

---

and information services. The decree also left extensive supervisory authority in the D.C. district court (Judge Harold Greene) to modify or lift any of these restrictions as competitive conditions warranted.

In his initial "triennial review" decision, Judge Greene left the bar on information services in place. *See* United States v. Western Elec. Co., 673 F. Supp. 525 (D.D.C. 1987). However, the Court of Appeals reversed that portion of his decision and remanded. *See* United States v. Western Elec. Co., 900 F.2d 283 (D.C. Cir.), *cert. denied sub nom.*, MCI Communications Corp. v. United States, 111 S. Ct. 283 (1990). Last July, on remand, Judge Greene reluctantly lifted the bar on BOC entry into information services. *See* United States v. Western Elec. Co., 767 F. Supp. 308 (D.D.C. 1991). Judge Greene stayed his own decision for a year to allow the opponents of BOC entry to appeal, but the D.C. Circuit lifted his stay, *see* United States v. Western Elec. Co., 1991–92 Trade Cases ¶69,610 (1991), and the Supreme Court let this action by the Court of Appeals stand, *see* American Newspaper Publishers Assoc. v. United States, 112 S. Ct. 366 (1991).

25. The Information Services Diversity Act of 1991, S. 2112, 102d. Cong., 2d Sess. (1991); *see* 137 CONG. REC. S18,438 (daily ed. Nov. 26, 1991).

26. The Telecommunications Act of 1991, H.R. 3515, 102d Cong., 2d Sess. (1991); *see* 137 CONG. REC. H7647 (daily ed. Oct. 8, 1991).

27. Testimony of Mitchell Kapor, President of Electronic Frontier Foundation, Before Subcomm. on Telecommunications and Finance, House Energy and Commerce Comm., Oct. 24, 1991, at 4.

tion providers? As Mr. Kapor stated in his testimony before the House Telecommunications and Finance Committee last October:

> It should be as easy to provide an information service as to order a business telephone .... Large and small [print] publishers coexist because everyone has access to production and distribution facilities—printing presses, typography, and the U.S. mails and delivery services—on a nondiscriminatory basis.[28]

Large and small information service providers similarly should be able to coexist.

Second, how can we promote wide and affordable access for users of the network? Such an objective requires that networks be interoperable.

Third, will new measures be needed to protect our citizens' right to privacy as more and more of their personal information is transmitted over public lines? In today's technologically sophisticated age, a great deal of private information is maintained by third-party custodians, such as banks, credit card companies, and direct marketing companies. That information, collected for one purpose, is increasingly being used for other, sometimes unrelated, purposes. In this context, the right to privacy takes on new dimensions.

Fourth, what changes to the Copyright Act will be required to develop adequate means of protecting the copyrights in information traveling over the network? In a world in which articles or whole books may be sent easily from computer to computer, we will have to take care to protect the rights of authors and publishers.

Fifth, how can the greatest degree of First Amendment freedom be assured for information flowing over the network? How do we distinguish between private and public communications? Does control of the medium justify control of the content? How do we distinguish between editing and censorship? And what if we face censorship not just by government but by network owners? Traditionally, different First Amendment standards have been applied to print, broadcast, and common carriers, with the greatest First Amendment protection extended to print. Which, if any, of these models is adequate to address the unique issues raised by developing communications?[29]

---

28. *Id.* at 8.

29. These questions concerning the application of First Amendment principles to electronic networks are addressed in more detail by Henry H. Perritt, *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65 (1992) (this issue).

As we move into the 21st century, information services will expand and broaden our access to valuable information resources. The diversity of these services will enhance the richness and depth of our free society.

III. FEDERAL WIRETAP STATUTE

My work in 1986 to enact the Electronic Communications Privacy Act ("ECPA")[30] involved an effort to examine new technologies in our existing legal framework. In this sense, it was a precursor to what would become the mission of the Technology Subcommittee. ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968[31]—the Federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill updated the 1968 law to clarify Federal privacy protections and security in light of new computer and telecommunications technologies. Oversight and, where necessary, updating of ECPA continue to be major focuses of the Technology Subcommittee.

When the framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers, and effects" protected by the Fourth Amendment.[32] During the intervening 200 years, development of new methods of communication and of devices for surveillance has expanded the opportunity for such intrusions dramatically.

When the Supreme Court first addressed the issue of government wiretapping in *Olmstead* v. *United States*,[33] it held that wiretapping did not violate the Fourth Amendment because there was no searching, no seizure of anything tangible, and no physical trespass. Today, the case is remembered more for Justice Brandeis' prescient dissent than for its holding:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be

30. 18 U.S.C. §§ 2510–2710 (1988). This Act incorporated and amended previously existing law.

31. 18 U.S.C. §§ 2510–2520 (1982).

32. U.S. CONST. amend IV.

33. 277 U.S. 438 (1928).

> that the Constitution affords no protection against such invasions of individual security?[34]

Forty years later, the Supreme Court accepted Justice Brandeis' logic in *Katz* v. *United States*,[35] holding that the Fourth Amendment applies to government interception of a telephone conversation. At the same time, the Court extended Fourth Amendment protection to electronic eavesdropping of oral conversations.[36]

Congress responded by authorizing government interception under certain circumstances in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[37] Title III remains the primary law protecting the security and privacy of business and personal communications today. Under the 1968 Act, protection of voice communications was expressly limited to the unauthorized aural interception of wire or oral communications; it applied only where the contents of a communication could be overheard and understood by the human ear. Furthermore Title III applied only to interceptions of communications sent via common carriers.

ECPA amended Title III to bring it in line with technological developments and changes in the structure of the telecommunications industry. It addressed the interception of wire, oral, and electronic communications, access to stored wire and electronic communications, and the use of pen registers and trap and trace devices.[38] The purpose of ECPA is to protect privacy interests while recognizing the government's legitimate law enforcement needs.

Six years after enactment of ECPA, we must again update Title III to cover developing technologies. Last year, I convened a task force of industry and civil liberties experts to examine developments in communications technology and to determine the extent to which ECPA protects those new technologies.[39] The task force considered new cellular phones, personal communications networks, new generations of cordless phones, wireless modems, wireless local area networks, and electronic

---

34. *Id.* at 474.
35. 389 U.S. 347 (1967).
36. Berger v. New York, 388 U.S. 41 (1967).
37. 18 U.S.C. §§ 2510–2520 (1982).
38. *See* 18 U.S.C. § 2511 (1988). Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. The same holds true for trap and trace devices, which record the numbers of telephones from which calls have been placed to a particular telephone.
39. Final Report of the Privacy and Technology Task Force. Submitted to Sen. Patrick J. Leahy, May 28, 1991.

mail and messaging. While the task force did not reach consensus on all of the issues it considered, it did agree that "traditional privacy principles, embodied in the Constitution, must guide public policy with respect to communications privacy and the new technologies."[40] This year, I am working on legislation that would update ECPA to address some of the recommendations made by the task force.

One issue on which the task force did not reach consensus was Caller-ID technology. In 1989, Senator Herb Kohl (D-Wisconsin) introduced legislation that would authorize Caller-ID as an exception to the wiretap statute's prohibition against trap and trace devices.[41] In 1991, the Senate Judiciary Committee approved a version of that bill, which would authorize Caller-ID, provided that the telephone companies offer customers the ability to block transmission of their phone numbers to the called party on a per-call basis.[42]

Caller-ID is the latest service to focus public attention on the effect of new technologies on our ability to control personal information. In our increasingly complex, technological, and interconnected world, preserving control over the private aspects of our lives is a great challenge. Every day we enter into transactions — with businesses and with the government — that require us to divulge personal information in order to identify ourselves. Providing that information to a third party reduces our control over its use, now and in the future.

Caller-ID has been controversial precisely because it raises questions about who has the right to determine whether consumers should be forced to put their phone numbers into the public realm. Senator Kohl's Telephone Privacy Act is an effort to address the competing interests involved in this debate. Congressional consideration of the Telephone Privacy Act is an important step in the evolution of U.S. privacy law. In the last two decades, Congress has expanded the legal protections for individual privacy in one context after another. These laws reflect the public's desire to shield from others information about themselves.[43]

I support the thrust of the Telephone Privacy Act because it provides

---

40. *Id.* at 2.

41. *See Caller-ID Technology: Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. (1990).

42. S. 652, 102d Cong., 1st Sess. (1991); *see* S. REP. NO. 247, 102d Cong., 1st Sess. (1991).

43. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) (1974); Privacy Act, 5 U.S.C. § 552a (1974); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1978); Cable Communications Policy Act, 47 U.S.C. § 551 (1984); Electronic Communications Privacy Act, 18 U.S.C. § 2510 (1986); Video Privacy Protection Act, 18 U.S.C. § 2710 (1988).

a minimum of privacy protection for Americans in all fifty states and in the District of Columbia. However, I do not support the provision in the bill that would preempt states from authorizing blocking on a per-line or subscription basis. Federal privacy laws typically provide a baseline that permits the states to afford additional protection where appropriate.[44] These laws take the correct approach by setting a minimum standard of protection on which a state can expand if it determines that greater privacy protection is appropriate for its citizens.

Notwithstanding the preemption provision, I supported the bill because it establishes a minimum of privacy protection as a prerequisite for offering the Caller-ID service. In addition, delaying the cut-off date for preemption until the date of enactment of the bill gives states time to decide whether to enact greater privacy protection.

IV. DIGITAL TELEPHONY

This year, we are examining a different wiretap problem posed by new technology.

According to law enforcement authorities, evolving telecommunications technology will make it increasingly difficult for them to intercept communications pursuant to a court authorized wiretap.[45] Last year, the Administration proposed a Sense of the Senate Resolution, which would direct electronic communications service and equipment providers to aid law enforcement officials in obtaining the plain text of voice or electronic communications after an appropriate warrant has been issued. That provision was originally included in anti-terrorism legislation, but was removed at my request.[46]

This year, the Department of Justice and the Federal Bureau of Investigation ("FBI") proposed legislation that would direct the Federal Communications Commission ("FCC") to issue regulations requiring the modification of existing equipment and the preservation of the government's ability to wiretap in the future. The proposal also permits

---

44. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (1982); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2710 (1988); Video Privacy Protection Act, 18 U.S.C. § 2710 (1988).

45. William S. Sessions, *The F.B.I. Needs Industry's Help*, N.Y. TIMES, Mar. 27, 1992, at A35; *see also* WASH. POST, Mar. 10, 1992, at C1.

46. S. 266, 102d Cong., 1st Sess. (1991) (reintroduced as S. 1241, 102d Cong., 1st Sess. (1991)).

the FCC to allow the phone companies to pass the costs of these changes on to consumers.[47]

This proposal has caused concern in the telecommunications, computer, consumer, and civil liberties communities. I am working with all interested parties to determine whether changing technology will frustrate the government's authority to conduct lawful surveillance and, if so, how Congress should address that problem.

Industry and civil liberties advocates have expressed additional concern because the government has also indicated that it would like Congressional help in dealing with the increased use of encryption devices by potential targets of law enforcement investigations. Those devices make it more difficult and expensive for the FBI to get court-authorized information that it currently obtains with little difficulty. I am concerned, however, that forcing equipment and service providers to give the FBI a trap door to any privacy or encryption features they offer would raise broad policy implications for computer security, trade, export controls, communications, and private business initiatives.

V. FREEDOM OF INFORMATION ACT

This year is the twenty-sixth anniversary of the Freedom of Information Act ("FOIA"). FOIA is no more and no less than a codification of the democratic principle that the public has the "right to know." The Technology Subcommittee oversees FOIA. Currently, we are working to ensure that technology will not render portions of that statute obsolete.

In 1966, FOIA established a statutory right of access to government records by any person who requested them.[48] It was, as John Moss said at the time, an "historic act."

In 1974, FOIA was amended to improve administrative procedures, to allow attorneys' fees for successful plaintiffs, and to authorize judges to review documents in camera to determine whether they were properly withheld.[49] The Watergate scandal, which culminated in President Nixon's resignation in August of that year, demonstrated the danger of secrecy in government. The public reaction to that scandal fore-

47. *See Oversight Hearing: FBI Authorization Request for Fiscal Year 1993 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 102d Cong., 2nd Sess. (1992) (testimony of FBI Director William S. Sessions).

48. 5 U.S.C. § 552 (1988).

49. *See* 94TH CONG., 1ST SESS., FREEDOM OF INFORMATION ACT AND AMENDMENTS OF 1974, SOURCE BOOK: LEGISLATIVE HISTORY, TEXTS, AND OTHER DOCUMENTS (Joint Comm. Print 1975).

shadowed the override of President Ford's veto of the FOIA amendments.[50]

In the early 1980s, the executive branch used every means at its disposal to clamp down on access to information. We fought fierce battles in those years, as the Administration worked hard to limit the scope of the Act and to curtail the public's knowledge of what the government was doing. In 1986, FOIA was amended to address certain law enforcement concerns and to change the fee structure.[51]

In its twenty-six years, FOIA has led to the disclosure of information on consumer health and safety; waste, fraud, and abuse in the government; foreign policy; civil and constitutional rights; and the environment. From revelations about the dangers of the Ford Pinto gas tank and red dye #2 to accidents at the Rocky Flats nuclear weapons plant, FOIA has informed us about serious threats to our health. In just the last few years, information on the Hubble space telescope and details of the savings and loan crisis were made available to the public through FOIA.

Today we find ourselves in a different world from 1966. As the government moves full force into the computer age, carbon paper and mimeograph machines have long since given way to computers, fax machines, and electronic mail systems.

What does that mean for the Freedom of Information Act? It should mean more access for people—like those with sight or hearing impairments—who have traditionally been excluded from meaningful participation in our system of government.[52] It should mean for FOIA what it has meant for the rest of the world—faster, cheaper, and more efficient communications. Unfortunately, this is not necessarily happening. Some agencies use computers to frustrate rather than to help information seekers, while others simply do not use computers efficiently.

The questions raised by electronically stored information technologies have been explored in several contexts.[53] Last year, the House of

---

50. *See* Veto Message, 10 WEEKLY COMP. PRES. DOC. 42 (1974); 120 CONG. REC. 36,633 (1974) (House overrode veto.); 120 CONG. REC. 36,882 (1974) (Senate overrode veto.).

51. Anti-Drug Abuse Act of 1986, Pub. L. No. 99–570, tit. I, subtit. N, §§ 1801–1804, 100 Stat. 3207 (1986) (codified at 22 U.S.C. § 2291 (1988)).

52. According to the American Foundation for the Blind, the availability of information in standard electronic machine readable form will greatly facilitate the expeditious and cost efficient production of such information in braille, large print, or synthetic speech output. Making the Federal Register available at reasonable cost in a form that is more compatible with braille, large print, or speech output is something our government ought to do to help ensure that all of us can participate more fully in the policymaking process.

53. ELECTRONIC COLLECTION AND DISSEMINATION OF INFORMATION BY FEDERAL AGENCIES: A POLICY OVERVIEW, REPORT OF THE COMM. ON GOVERNMENT OPERATIONS, U.S. HOUSE OF REPS., H. REP. NO. 560, 99th Cong., 2d Sess. (1986); U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMING THE NATION: FEDERAL INFORMATION DISSEMINATION IN AN ELECTRONIC AGE (1988);

Delegates of the American Bar Association approved a resolution encouraging agencies to ensure that "access to information under the FOIA not be diminished by virtue of the fact that the information is maintained in electronic form."[54]

In 1991, Senator Hank Brown (R-Colorado), ranking member on the Technology Subcommittee, and I introduced legislation to bring FOIA into the computer age.[55] While there is no question that FOIA covers all government information—regardless of its format—there are technical questions raised by the increased use of computers.

How do we define a FOIA search? Is an automated database search synonymous with looking through a file cabinet? My view is that it should be faster and easier for an agency to do. In this age of paper records and computer tapes, should requesters be given the format of their choice? My bill requires that if the requester's format of choice exists, the agency should make it available, and if it does not exist, the agency should make reasonable efforts to provide it.

My legislation also addresses the problem of delays. The single biggest complaint about FOIA is that requesters wait weeks, months, even years to get information from the government. While there is no question that agencies sometimes delay to avoid responding to a specific request, it is also true that in this age of budget deficits, lack of resources is a serious problem. I am proposing that we allow agencies to retain half of the FOIA fees they collect *if* they comply with the statutory time limits.[56] The fees they retain will be channeled back into the agency's FOIA operation. This incentive should alleviate some of the horrendous FOIA backlogs.

We must keep in mind that the purpose of FOIA is to make information available to the public—FOIA is a disclosure statute, not a withholding statute. In that context, many of these issues become clear. The government should do what it reasonably can to make information available to the American public.

Electronic Public Information and the Public's Right to Know, Proceedings of the Benton/Bauman Foundation Conference, Oct. 23–24, 1989.

54. 1990 A.B.A. SEC. ADMIN. L. & REG. PRAC. (Feb.)

55. S. 1940, 102d Cong., 1st Sess. (1991).

56. *See* 5 U.S.C. § 552(a)(6)(A) (1988) (statutory time limits).

VI. JOINT PRODUCTION VENTURES: THE NATIONAL COOPERATIVE RESEARCH ACT EXTENSION

One of my chief initiatives in the competitiveness area is the National Cooperative Research Act Extension, also known as the joint production bill.[57] This bill clarifies and eases antitrust restrictions on joint manufacturing and production ventures by bringing them within the scope of the National Cooperative Research Act of 1984 ("NCRA").[58] The NCRA codified the application of the rule of reason standard to joint research and development ("R&D") ventures. This standard requires a court to consider a joint venture's competitive benefits against allegations of anti-competitive effects. The NCRA also limited antitrust recoveries against joint R&D ventures that abide by the NCRA's notification procedures to single damages and attorneys' fees. The essence of the legislation is to extend these provisions of the NCRA from R&D joint ventures to production joint ventures.

The NCRA was designed to promote R&D by clarifying the applicability of the rule of reason standard and establishing a procedure under which firms may notify the Department of Justice and Federal Trade Commission of their cooperative ventures and thereby qualify for a single-damage limitation on civil antitrust liability.[59] The Act has been highly successful. Since its enactment, companies have filed over 230 notifications for joint R&D ventures involving everything from chipmaking and steelmaking processes to superconductors.[60]

Hearing testimony revealed the need for legislation that would extend the NCRA's protection of joint R&D ventures to joint production ventures. The capacity of American technological innovation remains unsurpassed. United States scientists and engineers continue to lead the way through scientific and technological breakthroughs that make new and better products possible. However, world technological leadership depends on the ability to convert R&D advances rapidly into commercial production.[61] Such production frequently requires large capital contributions and the investment of resources beyond the practical ability of any

57. S. 479, 102d Cong., 2d Sess. (1991); *see* 137 CONG. REC. S2263 (1991).

58. Pub. L. No. 98–462, 98 Stat. 1815 (1984) (codified at 15 U.S.C. §§4301–4305 (1988)).

59. *See generally* Daniel M. Crane, *Joint Research and Development Ventures and the Antitrust Laws*, 21 HARV. J. ON LEGIS. 405 (1984).

60. *See* S. REP. NO. 146, 102d Cong., 1st Sess. 2 (1991).

61. *See Legislation Concerning Product Joint Ventures, Hearing Before the Subcomm. on Antitrust, Monopolies and Business Rights of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. 137–38 (1990) (statement of David J. Teece).

one firm. This is especially true for small businesses.[62]

Almost a decade ago, the authors of the NCRA recognized that antitrust laws may inhibit procompetitive R&D joint ventures because of uncertain legal standards combined with the threat of treble antitrust damages. The Judiciary Committee emphasized the importance of clarifying antitrust uncertainty in the legislative history of the NCRA:

> The Committee concludes that valuable joint R&D activity has been discouraged by the paucity of clear legal guidelines about the application of the antitrust laws to this type of activity. The perception by many firms of exaggerated antitrust risks will continue to deter desirable joint activity unless Congress acts to clarify the essential difference between joint activities and the kind of collusive conduct that is properly condemned by the antitrust laws. The Committee intends by adoption of this bill to eliminate, or at a minimum lessen, any perception that the antitrust laws deter competitive joint R&D activity . . . .[63]

Critics of the joint production bill contend that there is no need for new legislation clarifying antitrust uncertainty regarding joint production ventures.[64] However, as Assistant Attorney General Rill has stated, notwithstanding more recent trends in antitrust analysis, the existence of older precedent less favorable to joint production ventures unnecessarily and significantly chills much procompetitive conduct:

> Our antitrust laws rely on private as well as public enforcement, however, and the fear of a private action for treble damages can be a powerful deterrent to procompetitive conduct where uncertainty exists regarding the applicable antitrust standards. Recent trends in antitrust analysis are more favorable to procompetitive joint ventures, but older precedent applying very strict rules to joint ventures between competitors may still lead antitrust practitioners to give conservative advice to avoid treble damages, and, we believe, still lead firms to reject participation in joint ventures that would not be

62. *See id.*

63. S. REP. NO. 427, 98th Cong., 1st Sess. (1984).

64. *See, e.g., Hearing Before the Subcomm. on Antitrust, Monopolies and Business Rights of the Senate Comm. on the Judiciary, supra* note 61 (statement of Dr. Joseph F. Brodley).

anticompetitive.[65]

Such uncertainty poses a significant obstacle to pooling resources necessary to convert innovation into finished product. For example, as the late Dr. Robert Noyce, President of SEMATECH, Inc., testified before the Subcommittee on Technology and the Law:

> Small companies cannot get the economy of scale on a world-wide basis enjoyed by the established companies unless they pool their resources and participate in joint manufacturing. Our antitrust laws make such participation very impractical due to the real or perceived risk of treble damages.[66]

Under more recent precedent, production joint ventures are already subject to the rule of reason analysis by the courts or the reviewing federal agency.[67] However, the joint production bill eliminates any lingering doubt by amending the National Cooperative Research Act to codify that production joint ventures shall not be deemed per se illegal. In this way, any antitrust uncertainty that may have impeded the formation of desirable, procompetitive joint ventures will be greatly reduced.

The legislative history of the NCRA described in some detail the proper application of the rule of reason standard by the courts and the federal agencies in analyzing the competitive effects of a challenged R&D joint venture.[68] As was noted in the 1984 legislative history, the rule of reason condemns only those joint ventures whose anticompetitive effects outweigh procompetitive merits. If anticompetitive effects are established, the court must weigh them against any demonstrated procompetitive effects in determining whether an antitrust violation has occurred.[69]

Much of our national inventive dynamism—particularly in the field of high technology—is located in our small enterprises.[70] If small firms can maintain their small-unit innovative capacity and yet join with other firms for R&D and manufacturing when a project is too sizeable, costly,

---

65. *Id.* at 17 (statement of James F. Rill).

66. *Joint Ventures in the Semiconductor Industry, Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. 17 (1990) (statement of Robert N. Noyce).

67. *See, e.g.*, United States v. Penn-Olin Chem. Co., 378 U.S. 158 (1964).

68. S. REP. NO. 427, 98th Cong., 2d Sess. 17–19 (1984).

69. *See id.* at 19.

70. *See, e.g., Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, supra* note 66, at 24–25 (statement of Sanford Kane); *id.* at 33–35 (statement of Gary Hillman).

or risky to do alone, the entire nation will benefit. This legislation will enable small businesses and individual investors to assist each other in the manufacturing of new technologies.

In testimony before the Antitrust Subcommittee, Prof. David Teece, Director, Center for Research and Management, University of California at Berkeley, emphasized that this legislation would not encourage mergers and industry concentration. Instead, it would allow small- and middle-sized firms to maintain their independence and yet join with other companies for R&D and production.[71]

Assistant Attorney General James F. Rill concurred that an extension of the NCRA would be beneficial to small companies: "Smaller firms may benefit particularly from the ability to achieve these sorts of efficiencies through a joint production venture."[72]

Mr. Mitchell E. Kertzman, President of Powersoft Corp., a software firm located in Burlington, Massachusetts and employing 151 people, testified before the Antitrust Subcommittee on behalf of the American Electronics Association, which represents over 3,000 U.S. high-tech companies, and the Coalition for Joint Manufacturing, an informal coalition of nine associations, representing more than 200,000 individual member companies and over ninety percent of all U.S. manufacturing. He represents the views of both small and large businesses in his analysis of the proposed legislation:

> We share the concern of Mr. Porter and the Chairman about the merger mania that seems to be sweeping the nation. However the bill under consideration has nothing at all to do with mergers and acquisitions. It has everything to do with encouraging limited strategic partnerships among companies to enable them to share the risks and commercialize specific advanced technologies.[73]

In sum, this legislation was carefully crafted to respond to the growing pressures generated by technological advances and international competition without risking harm to the competitive marketplace or to the integrity of our antitrust laws. While I do not believe that this bill is a panacea for our nation's current economic woes, I do believe it will remove a significant impediment to our international competitiveness.

---

71. *Id.* at 137–38 (statement of David J. Teece).
72. *Id.* at 24 (statement of James F. Rill).
73. *Id.* at 209 (statement of Mitchell E. Kertzman).

VII. COMPUTER VIRUSES

Another area in which I am particularly interested is legislation regulating computer security. The importance of such legislation was recently underscored by the discovery of the so-called "Michelangelo" computer virus in computer systems throughout the public and private sectors.[74] Although the issue has received a great deal of press recently, the potential threat of viruses and other destructive breaches of computer security has existed for some time. The Subcommittee on Technology and the Law has worked over the past three years to draft balanced legislation aimed at addressing this problem.[75]

The latest result of these efforts is the Computer Abuse Amendments Act (the "computer virus bill"), which is included as a title to the Violent Crime Control and Enforcement Act.[76] The computer virus bill updates the Computer Fraud and Abuse Act ("CFAA").[77] It addresses changes in computer technology, particularly new computer abuse techniques such as computer viruses, worms, and Trojan Horses, which make prosecutions difficult in some types of cases. The computer virus bill clarifies the intent standards and the actions prohibited. These improvements will benefit both computer users and law enforcement.[78]

The maintenance of the security and integrity of computer systems has become increasingly critical to interstate and foreign commerce, communications, education, science, technology, and national security. As we move even further into the hi-tech age, we depend on computers to process essential information and to store it in a manner in which it will not be altered.[79] The deliberate abuse of computers and computer systems to cause damage, disruption, and interference with computer operations has already posed significant burdens on numerous computer users. And the problem knows no international boundaries.

The computer virus bill creates a structure for treating such

---

74. *See, e.g.*, John Burgess, *"Michelangelo" Scare Stirs Fears About Computer Viruses*, WASH. POST, Feb. 17, 1992, at A1.

75. *See Computer Viruses, Hearing Before the Subcomm. of Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 1st Sess. (1989); *The Computer Abuse Amendments Act of 1990, Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 101st Cong., 2d Sess. (1990).

76. *See* H.R. 3371, tit. 27, 102d Cong., 1st Sess. (1991); *see also* S. REP. NO. 405, 102d Cong., 1st Sess. (1991). The House of Representatives passed the conference report on H.R. 3371 on Nov. 26, 1991. *See* 137 CONG. REC. H11,884 (daily ed. Nov. 26, 1991). As of this writing, the Senate has yet to close debate on the conference report.

77. 18 U.S.C. § 1030 (1988).

78. *See* 137 CONG. REC. 8918 (daily ed. June 27, 1991).

79. *See, e.g., Hearing Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary, supra* note 75, at 1 (statement of Senator Leahy).

incidents — whether they are intentional, malicious, accidental, or reckless — with appropriately balanced legal sanctions.

The bill broadens jurisdiction for newly created sections of the Computer Fraud and Abuse Act, to cover all computers used in interstate commerce or communications. It is the intent of the legislation to exercise the full extent of Congress' constitutional powers under the commerce clause to prohibit forms of computer abuse that arise in connection with, and have a significant effect on, interstate or foreign commerce.[80]

A primary focus of the legislation is to avoid the complications and ambiguities created by certain language in the current CFAA. Computer abuse crimes under the current statute must be predicated on the violator's gaining "unauthorized access" to the affected Federal interest computers. However, as demonstrated by several recent computer abuse incidents, the most severe forms of computer damage are often inflicted on remote computers to which the violator never gained "access" in the commonly understood sense of that term. Instead, as in the case of Michelangelo, those computers are damaged when a malicious program or code is replicated and transmitted by other computers or diskettes already infected by a violator's earlier transmission of a virus.

The new subsection 1030(a)(5) of the CFAA created by the computer virus bill makes it clear that one who transmits a destructive program or code with harmful intent is criminally responsible for the resultant damage to all affected computers, without regard to the element of "unauthorized access." The new provision places the focus on harmful intent and resultant harm, rather than on the technical concept of computer "access."

The computer virus bill also creates a new civil remedy for those harmed by violations of the Computer Fraud and Abuse Act. This remedy would boost the deterrence effect of the statute by allowing aggrieved individuals to obtain relief in a private cause of action.

CONCLUSION

Technology is moving us rapidly into the next century. My goal is to encourage the new technology that will improve our international competitiveness, our domestic businesses, and our daily lives. But we cannot sacrifice the principles that bind this country together on the altar of technological progress. Ours is a nation of laws, established on pro-

80. *See* S. REP. NO. 544, 101st Cong., 2d Sess. (1990).

found principles of freedom. That framework guides, but does not restrain us as we move into the future.