

September 26, 2001

The Honorable Ernest F. Hollings
Chairman
Senate Committee on Commerce, Science, and Transportation
SR-254 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Hollings:

We recently learned that you intend to introduce legislation to require computer and electronics manufacturers to include digital watermark technology or other copyright-protection technologies in the production of certain products and multi-use devices. As the Co-Chairs of the U.S. Public Policy Committee of the Association for Computing Machinery (ACM), we are writing to express our deep concern regarding the potential legislative proposal known as the Security Systems Standards and Certification Act (SSSCA).

As Congress considers legislation with respect to the use of copyrighted works on the Internet and in other digital and electronic contexts, we urge you to recognize that there are many legitimate uses of technology that would be impaired by additional copyright-protection measures. Enacting additional copyright-protections beyond those already provided by the Digital Millennium Copyright Act (DMCA) is unwarranted. Already, we have seen an unintended chilling effect on computer security research by the DMCA. Any law along the lines of the SSSCA might well have more far-reaching and damaging effects, particularly as our nation attempts to enhance the security of our infrastructure and prevent acts of terrorism.

We would ask that you carefully consider the issues of cost, liability, and government interference in technology standards-setting that would be imposed by this legislation. We can think of many objections to the legislation, based on our reading of the draft bill.

Here is a small sampling:

- Colleges, universities and trade schools throughout the U.S. would no longer be able to teach advanced computer science and computer engineering.
- The acts of writing basic operating system software or assembling simple computer systems in classes or as assignments would be against the proposed law.
- Research in computer security and protection would be further curtailed, as any such research would be required to be done on (and not interfere with) whatever technology is imposed by this law. However, malicious actors do not need to be so concerned. This has significant national security implications.

- Researchers and hobbyists seeking new uses for innovative technology might well find their experimentation and prototypes to be criminal under this law.
- Devices as disparate as electronic cameras, wrist watches, electric pianos, televisions, ATM machines, cell phones, home security systems, and medical equipment (among many examples) all process and display information electronically. Under the proposed legislation, all would be required to support anti-copying protocols. In most such cases, this is absurd and will raise costs unnecessarily. Inclusion of anti-copying technology in general purpose equipment -- including real-time computing devices used in traffic control, air flight control, medical equipment, and manufacturing -- adds to their complexity and potential for failure. Unexpected interactions with other code, and accidental activation of protection protocols cannot be ruled out in every case, and in many venues the potential for damage is extreme.
- Photocopy machines, telephones and VCRs are now digital in form and can copy information. Forcing adoption of anti-copying protocols on those machines will change accepted modes of use, at best, and may render them unusable for their intended purposes.
- Other countries will not have similar requirements in their laws and may actively fear the imposition of anti-copy technologies; this will put U.S. products at a competitive disadvantage with other products manufactured elsewhere in the world. At a time when electronics manufacturers in other countries are seeking an advantage over U.S. firms, this could be catastrophic for the U.S. electronics industry. In addition, the draft version of SSSCA would have significant negative impacts on foreign technology imports, such as the linux operating system, in direct violation of our obligations as a participating member of the World Trade Organization.

As a publisher of electronic media, ACM is acutely aware of the problems with copyright protection in the modern world. However, as technologists, we also believe that the solution is not to be found in constraints and prohibitions on the technology. Rather, there needs to be more efforts made in enforcement of current laws, in education of consumers, and in deriving new models for e-commerce. Historically, the entertainment and publishing industries have claimed potential ruin from new technologies. However, those new technologies (such as videotape) have actually served to increase the consumer demand and income for those industries once the technologies were embraced.

In our society, we have achieved technological excellence, research leadership, and educational preeminence in the world through the free exchange of information and the freedom to innovate. Copyright was intended to support those goals, not restrict them for entertainment companies. The explicit embodiment of "fair use" provisions in the law has contributed to our many successes. Any further legislative action -- such as the SSSCA -- which focuses on constraining or outlawing technology instead of penalizing behavior

can only serve to weaken our educational systems, impede our technological dominance, and interfere with our electronic security.

Comprised of computing professionals from academia, industry, and government, the U.S. Public Policy Committee of the Association for Computing Machinery is pleased to offer our technical expertise to assist policy makers in the development of computing and information technology policy. We would appreciate the opportunity to testify before the Senate Committee on Commerce, Science and Transportation Committee on technology policy matters, including proposals to require manufactures to include copyright-protection technologies in products and multi-use devices. Please contact Jeff Grove, Director of the ACM Public Policy Office at (202) 659-9711, if you have any questions or if we can be of assistance to your efforts.

Sincerely,

Barbara Simons, Ph.D.

Eugene H. Spafford, Ph.D.

Co-Chairs

U.S. ACM Public Policy Committee (USACM)

Association for Computing Machinery