

**LEX TECHNICA: MATHEMATICIANS SPEAK**  
**by Laura Jennings (GCN)**

Can the Pythagorean theorem be illegal? If a mathematical expression is part of a software code that is designed to unlock encrypted, copyright-protected information, the expression may be a violation of law. However, while  $a^2 + b^2 = c^2$  may be illegal, the statement that the square of the hypotenuse of a right triangle is equal to the sum of the square of its sides may be just fine. How can this be? Congress enacted the Digital Millennium Copyright Act (DMCA), which among other things, outlaws the selling of any device, to include software source code, that circumvents a technological measure employed to control access to a work. Court decisions indicate that posting code to the net is equivalent to trafficking in a circumvention device under the DMCA. This means that the communication or dissemination of information which can be used to unlock protected information may subject the author and the disseminator to civil and criminal penalties. Does this prohibition on expression of information violate the First Amendment?

Making their way through the courts are several cases, which involve the constitutional collision of free speech, copyright, and digital access technology. The cases are split on the scope of the application of the First Amendment to software code and the issue is likely to end up in the U.S. Supreme Court. Software code is the lifeblood of the information technology revolution, but is it more functional than expressive? Digital information is now both the property which is protected as well as the means used to lock and unlock the property. The tools to open and shut the security doors can be characterized as trade secrets, a form of creative expression and a communication of ideas. Copyright owners seek to control the tools as a way to protect commercial information. Software engineers are claiming that their work about encryption is protected by the First Amendment. This article will explore the sovereignty of code in cyberspace and examine cases involving the application of copyright law and the First Amendment to technological encryption measures.

Not all speech is equal under the First Amendment. There is precedent in the Supreme Court to extend different levels of protection to speech depending on the nature of the speech and the type of regulation which is suppressing the speech. Free speech is not an absolute right; for example, obscenity, commercial speech and speech which incites imminent unlawful behavior can all be regulated. In FCC v. Pacifica, 438 U.S.

726 (1978), the Court ruled that the Government was able to regulate the broadcast times of the George Carlin monologue, "Filthy Words." In U.S. v. Progressive, Inc., 467 F. Supp. 990 (1979), the Court enjoined publication of the article, "The H-Bomb Secret: How We Got It and Why We're Telling It." In order for a court to impose a prior restraint on speech, the plaintiff must be able to show that irreparable harm will occur unless the speech is enjoined. Where does Government control of software fall in this continuum? When can digital speech be regulated? Should software source code receive strict protection under the First Amendment? Does a computer programming language deserve the same constitutional protection as political or artistic speech? Is creating a software virus protected under the First Amendment or is it aiding and abetting a crime? How does one defend against a virus without researching and understanding a virus? How can one do research and openly discuss the findings but not be able to post the code itself? If the effect of software 'speech' is both to innovate and to potentially harm a commercial interest, what values should prevail?

To understand the momentous nature of the issues in the balance, one should be acquainted with a concept explored by Lawrence Lessig in his book, Code and Other Laws of Cyberspace. Lessig's principle is that in society, in this case cyberspace, the architecture controls the power. The code of the systems determines what can be done and how it can be done, and, if we are not careful, code can be a threat to liberty. In a digital communication network, programming code acts as a regulator of speech, property and human interaction. Code dominates through its control of structure. Thus, if code is the basis for the new means of production, in order to maintain digital diversity in information, technology and ideas, the role of Government is to maintain the greatest capability to create and publish code and to ensure that regulations over code enable the values of a democratic society.

The issue of the application of the First Amendment to software code and programs has been litigated in several cases. In Bernstein v. U.S. Department of Justice, 192 F.3d 1308 (1999), the U.S. Court of Appeals for the Ninth Circuit ruled that Government restrictions on publishing an encryption program on the Internet violated the First Amendment. At the time of the trial, encryption software, including both source code and object code, was regulated under the Export Administration Regulations (EAR) Commodity Control List for national security reasons. In a related case addressing the posting of encryption code on the Internet, Junger v. Daley, 209 F.3d 481

(2000), encryption software was viewed as expressive for First Amendment purposes and thus entitled to the protections of the prior restraint doctrine. In Junger The U.S. Court of Appeals for the Sixth Circuit ruled that the First Amendment protected computer source code and that posting on the net was an "export" under the EAR. In both Bernstein and Junger, the court recognized that its decision was limited to the facts of the case and was not a sweeping ruling about the Government regulation of software; what is presently unclear is what standard of review should be applied to First Amendment challenges to Government regulation of software. What is fueling this debate is whether software is primarily expressive or functional, and whether or not the regulations limiting expression of code are primarily affecting the content or functional aspects of the program. From a systems engineering point of view, code can control both content and function and the two work together inseparably because choices made with respect to function can have an effect on availability of content, and choices made with respect to content can affect decisions about functionality.

In order to address the potential commercial harm that the combination of digital technology and global communications can have to digital content owners, Congress enacted the DMCA as implementation of portions of the World Intellectual Property Organization Treaty (WIPO) (1997). WIPO signatories must provide adequate legal protection against circumvention of technological measures used by authors to restrict access to copyrighted works. The DMCA outlaws both conduct and devices which circumvent such measures. Circumventing a work is to descramble, decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the consent of the copyright owner. (17 USC 1201(a)(1)). Additionally, the DMCA provides that no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure. (17 USC 1201(a)(2)) It should be noted that the prohibitions do not apply to information security, intelligence or law enforcement activities.

The DMCA also allows reverse engineering for the purpose of achieving interoperability. The definition of interoperability is limited in scope to analyzing elements of independently created computer programs necessary for achieving interoperability when those elements have not otherwise been

made available. Thus, if a copyright owner makes an interface available, the right to examine the underlying code may be restricted. What the DMCA has effectively done is to shift the balance between copyright owners and the public domain by making it illegal to access a work unless that access is pursuant to specific proprietary hardware systems or contract terms. Under the DMCA security means protection from the user instead of security for the user. However, despite the new legal and technical restrictions, accessing a work in an unauthorized manner can still be technically accomplished; thus the enforceability of the DMCA will be an interesting cyberspace adventure.

Computer program engineers as well as energized hackers demonstrate that if security is dependent on digital information, then breaches of security occur through the application of additional digital information. The tension surrounding the control of information exists on many fronts: the Government has attempted to control technology so that criminal communication can be detected; copyright owners want to control access and use of information with commercial value; and, consumers want fair use and free access to information that they have purchased. The First Amendment can become an issue if the Government restricts people from writing computer programs which can either lock or unlock digital information. The Government can regulate speech, but any attempt to do so must pass scrutiny and reflect the kind of free society the Constitution seeks to maintain. As capability to publish information increases with networked computers, the means to control information content are likely to move from encryption measures to trusted systems.

The headlining DMCA case is Universal City Studios v. Corley, 273 F. 3d 429 (2001), in which the Second Circuit Court of Appeals upheld the lower court injunction against the defendants from posting or linking to the source code of DeCSS, a program to unscramble the film industry-supported Content Scrambling System (CSS) used to encrypt DVD movies. CSS-protected movies can only be viewed on DVD players which have the decryption keys embedded into the DVD player system. The DVD players allow you to play but not copy or change operating platforms. CSS was reverse-engineered by several programmers and the decryption program, DeCSS, was implemented by a Norwegian teenager and acts as a key to unlock the scrambled movie. DeCSS allows a DVD owner to play a DVD movie on a machine without the decryption keys as well as make copies of the DVD movie. DeCSS facilitates both legal and illegal acts

under pre-DMCA copyright law. Corley posted the DeCSS program and links to other versions of the DeCSS algorithm on his website. It should be noted that the DeCSS algorithm facilitates conduct which was considered legal prior to the passage of the DMCA. For example, court decisions have held that it is permitted to access and copy a work for the purpose of accessing those portions of a work which are not protected by copyright. Under the DMCA permissible access as well as copying has been limited.

The Court rejected several defenses to the injunction against posting and linking: the reverse engineering defense was rejected because the purpose for posting was not to solely achieve interoperability, and because the reverse engineering exception only applies to computer programs and not movies; the encryption defense was rejected because there was no showing of a good faith effort to do encryption research. In the lower court, the fair use defense was rejected because the defendants were not being sued for copyright infringement but rather for trafficking in a circumvention technology. The Appeals Court noted that the fair use defense has never included a guaranteed right to access to a particular format or technique. If the case goes to the Supreme Court, the minimization of fair use and the potential for a permanent lock on copyrighted information as well as locked but non-copyrightable information under the DMCA may be an issue. The defendants also argued that DeCSS technology had substantial non-infringing uses that were permitted under Sony Corp. v. Universal Studios, 464 U.S. 417 (1984), in which the Supreme Court held that private, noncommercial use of a VCR was a non-infringing fair use of a copyrighted show, when the purpose was time-shifting the viewing of taped programs. This analogy to VCRs was defeated because the DMCA outlawed circumvention technology and the VCRs in Sony did not have anti-circumvention technology. On appeal, the Court stated that the DCMA prohibitions were not directed at use but rather at circumvention of the lock. The response argument is that the lock minimizes legal uses, such as access to information unprotected by copyright but locked by encryption.

Most importantly, the Court addressed the application of the First Amendment to computer code and the constitutionality of the DMCA. When a court evaluates a challenge to a law or regulation as violating the First Amendment, the court must first decide whether or not the information is speech and then whether the regulation is content neutral. Content-based restrictions must be narrowly tailored to serve a compelling Governmental interest and use the least restrictive means

possible, while content-neutral regulations need only reasonably advance a substantial state interest. In a First Amendment legal challenge, the real fight is over the characterization of the regulation or statute. If a regulation is characterized as content-neutral, the regulation has a good chance of being upheld.

The Court addressed the First Amendment issue by stating that the computer code was speech - both expressive and functional - but that the program code was overwhelmingly functional; and because the DMCA was only targeting the functional aspects of the speech, the DMCA was content neutral. Specifically, the injunction was constitutional because it only covered the executable program and not discussions of the code. The Court reasoned that the causal link between the dissemination of circumvention computer programs and their improper use warrants selection of a level of constitutional scrutiny based on the programs' functionality. The Court seems to ignore the fact that a discussion of code using the actual code in the discussion would be an expressive communication. System engineers fluent in computer programming language may believe that source code is the most efficient and specific means to communicate ideas about cryptography. However, the Court also reasoned that the availability of an executable program on the Internet was closer to conduct than to speech in the speech-conduct continuum. (See, e.g., Clark v. Community for Creative Non-Violence, 468 US 288 (1984), in which a National Park Service regulation prohibiting camping in certain parks was found not to violate the First Amendment when applied to prohibit demonstrators from sleeping in Lafayette Park and the Mall in connection with a demonstration intended to call attention to the plight of the homeless.)

In another Supreme Court First Amendment case involving information technology, Turner Broadcasting System v. Federal Communications, 114 S. Ct. 2445 (1994), the Court held that the FCC requirement for cable television system operators to carry local broadcast stations constituted a "content-neutral" regulation that furthered an important Governmental interest and did not unnecessarily restrict the freedom of speech. In Turner, the Court stated that the distinction between cable operators and broadcasters was based upon the manner in which the speakers transmitted their message and not upon the messages themselves. The strong dissent argued that the regulation was not content neutral: Because there were limited channels and because the cable operators had to drop some programs, a selection was necessary and that selection was based on content.

The issues of whether or not source code is pure speech and whether or not regulations suppressing code are content-neutral or content-based will continue to be litigated. One California state appellate court has found DeCSS to be pure speech:

"Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSS encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were 'compiled' to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas. That the source code is capable of such compilation, however, does not destroy the expressive nature of the source code itself. Thus, we conclude that the trial court's preliminary injunction barring Bunner from disclosing DeCSS can fairly be characterized as a prohibition of 'pure' speech." DVDCCA v. Bunner (Cal. Court of Appeal, 6th Appellate District, November 2001).

How will the Supreme Court resolve the tension between the First Amendment and regulation of software code? It may be that the Court critically evaluates the underlying interest that the regulation is protecting. Software code is part of many different aspects of society. For example, the DMCA is protecting commercial information interests as opposed to physical harm to persons or infrastructure and therefore the Court may apply strict scrutiny to the regulation. The other difficulty in the issue of software regulation is enforcement. In the DMCA case, there was evidence presented that the decryption algorithm could be expressed in several ways; the executable version was the version enjoined. If the expressions of the algorithm not in a machine ready executable form are not enjoined, then the capability to decrypt is one step away. Objects which may be represented differently but which have the same essential structure are often said to be identical up to an isomorphism. (<http://mathworld.wolfram.com/Isomorphic.html>) When it comes to the expression of digital information, suppression of one version leaves the door open to infinite isomorphic statements. Censorship of alternative methods of equivalent expressions will exhaust law enforcement unless law enforcement increases technological policing of the net. Simultaneously, there is a significant paradigm shift occurring: computers are user-programmable and therefore the creation of technology which enables users to manipulate content is a wave with unstoppable momentum. We are approaching global samizdat.