Case No. 00-9185

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

UNIVERSAL CITY STUDIOS, INC., *et al.*

Plaintiffs-Appellees

v.

ERIC CORLEY, A/K/A EMMANUEL GOLDSTEIN AND 2600 ENTERPRISES, INC.

Defendants-Appellants

SHAWN C. REIMERDES, ROMAN KAZAN

Defendants

On Appeal From The United States District Court
For The Southern District Of New York

BRIEF OF *AMICI CURIAE*

**DR. STEVEN BELLOVIN; DR. MATT BLAZE; DR. DAN BONEH; MR. DAVE DEL TORTO;
DR. IAN GOLDBERG; DR. BRUCE SCHNEIER; MR. FRANK ANDREW STEVENSON;
DR. DAVID WAGNER**

IN SUPPORT OF APPELLANTS AND REVERSAL OF THE JUDGMENT BELOW

JENNIFER STISA GRANICK, ESQ.
California State Bar Number 168423
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-0014

Counsel for *Amici Curiae*

January 26, 2001

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTERESTS OF AMICI[1]

All parties have consented to the filing of this brief. FRAP 29(a).

The *amici curiae* are cryptographers, individuals whose work or hobby involves research, design, analysis, and testing of encryption technologies. *Amici* are concerned that Section 1201 of the Digital Millennium Copyright Act (“DMCA”), as construed by the District Court, too narrowly circumscribes cryptographers’ speech, research, teaching, and engineering activities whenever they involve computer code. Erroneously characterizing programming language as “functional,” the district court denied it the First Amendment protection it demands. Instead, the district court’s opinion would deprive cryptographers of the most effective language in which to communicate their research and its results, with the effect of weakening security systems and technological protection of data for the public.

Dr. Steven M. Bellovin is a member of the Internet Architecture Board and a leading expert on cryptography and Internet security. He holds several patents and has published numerous papers in these fields, including several papers that

[1] Affiliations are listed only to identify the amici, whose views expressed herein do not necessarily represent those of their respective employers.

demonstrate flaws in proposed or deployed cryptographic systems. Dr. Bellovin received a B.A. degree from Columbia University, and an M.S. and Ph.D. in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create netnews, for which he was co-awarded the 1995 Usenix Lifetime Achievement Award. He joined AT&T Bell Laboratories in 1982. Despite the fact that he has not changed jobs, he is now at AT&T Labs Research, working on networks, security, and why the two don't get along. He was named an AT&T Fellow in 1998. Bellovin is the co-author of the recent book *Firewalls and Internet Security: Repelling the Wily Hacker*.

Dr. Matt Blaze is a research scientist at AT&T Laboratories, where he studies the use of cryptography in computing and network security. His research focuses on the architecture, design and analysis of secure systems and on discovering new cryptographic primitives and techniques. He invented the field of “trust management,” a unified approach for specifying and controlling security policy in complex distributed systems, and leads the KeyNote project at AT&T Laboratories. He is responsible for a number of important cryptologic concepts, including Remotely-Keyed Encryption, Atomic Proxy Cryptography, and Master-Key Cryptography. Blaze's research has also been influential in network-layer encryption (he co-designed “swIPe,” a predecessor of the IPSEC standard for protecting Internet traffic), session-layer encryption, and filesystem encryption.

Blaze has discovered weaknesses in a number of published and fielded security systems, including the protocol failure in the U.S. Government's "Clipper" key escrow system that led to its abandonment. Blaze has been long been a leader in the debate on encryption and computer security policy, having testified before Congress several times and having led and participated in a number of influential public-policy panels and reports. He holds a Ph.D. in Computer Science from Princeton University.

Dr. Dan Boneh is a Professor at the Department of Computer Science at Stanford University. His research focuses on cryptography, specifically the security of cryptographic primitives and their application in real world systems. At Stanford he is leading a number of systems security projects on topics such as intrusion tolerance and security applications for handheld devices.

Mr. Dave Del Torto's career in Internet privacy and security started in the late 1980s at the University of California at Berkeley, where he was one of the original "Cypherpunks." He joined Pretty Good Privacy Inc. (PGP) as a founding employee in 1996, and in 1997 was part of the four-man team that published the entire PGP source code in 13 paper volumes, which resulted in the first legal international PGP freeware (exports of 128-bit encryption have since been greatly deregulated). He currently serves as the Executive Director of the CryptoRights

Foundation (a human rights security organization) and is the Chief Security Officer of MEconomy, Inc., a privacy infomediary company based in San Francisco.

Dr. Ian Goldberg received his Ph.D. in the area of Computer Security from the University of California, Berkeley, where he was a founding member of that university's Internet Security, Applications, Authentication and Cryptography research group. Dr. Goldberg is currently Chief Scientist of Zero-Knowledge Systems, where his research involves encryption, security, and privacy. He is well-known for uncovering critical security flaws in widely-deployed systems, including an early version of Netscape Navigator, and the GSM digital mobile phone. standard

Dr. Bruce Schneier is an internationally-renowned security technologist and author of six books, including *Applied Cryptography*, the seminal work in its field, and *Secrets & Lies: Digital Security in a Networked World*. Schneier has presented papers at many international conferences, and he is a frequent writer, contributing editor, and lecturer on the topics of cryptography, computer security, and privacy. Schneier served on the board of directors of the International Association for Cryptologic Research, and is an Advisory Board member for the Electronic Privacy Information Center. Schneier holds an MS degree in computer science from American University and a B.S. degree in physics from the

University of Rochester. He is an author of one of the five encryption methods considered as a finalist to become the United States' Advanced Encryption Standard. Currently he is currently the chief technology officer of Counterpane Internet Security Inc., which he co-founded.

Mr. Frank Andrew Stevenson is a Senior Researcher at Funcom Oslo, a leading developer of interactive entertainment. He does consulting in the field of cryptography and computer security. He has contributed to the field by publishing, on the Internet, both textual and source code descriptions of findings of flaws in Microsoft Windows 95's password protection, and likewise was the first to publish details of weaknesses in the CSS system. At trial he testified as a fact witness.

Dr. David Wagner is an Assistant Professor at the University of California at Berkeley's Computer Science Department. His research includes computer and telecommunications security, cryptography, privacy, anonymity, and electronic commerce. In September 1995, he and a colleague reported serious flaws in the techniques used for encrypting credit card numbers in the leading products facilitating the implementation of electronic commerce over the Internet. This discovery was reported on the front page of the *New York Times*, the front page of the business section of the *Washington Post*, and elsewhere.

SUMMARY OF ARGUMENT

Computer code is expressive speech essential to scientific exploration and communication among cryptographers, speech on which the District Court's injunction imposes an unjustified restriction. Thus Section 1201's purported prohibition on decryption code is properly analyzed with strict scrutiny. The DMCA's vague, content-based anticircumvention provisions fail even intermediate scrutiny, however.

The statutory "encryption research" exception of Section 1201(g) does not alleviate the harms to *amici*. In the cramped interpretation of the District Court, the "good faith encryption research" exception applies to virtually no one. The criteria and "factors" in determination of its applicability arbitrarily restrict those who may discuss encryption technologies and set unconstitutional prior licensing conditions on speech. Even cryptographers whose own speech is not restricted by Section 1201's provisions will be hampered by the inability to receive the communications of those who are chilled by the statute.

Amici propose a reading of Section 1201 more tailored to fit the statute's language and the demands of the First Amendment. Specifically, *amici* contend that 1201 cannot apply to enjoin the publication and dissemination of a computer program unless the standards of strict scrutiny under the First Amendment, as well as the procedural protections applicable to injunctions under the First Amendment, have been met.

ARGUMENT

I. Section 1201 Reaches a Broad Range of Cryptographers' Activity

Gabriel García Márquez sets *One Hundred Years of Solitude* in a time when " The world was so recent that things lacked names, and in order to indicate them it was necessary to point."[2] The science of cryptography has moved well beyond the pointing stage, but the district court's opinion would return us to that primitive level by denying cryptographers the right to communicate in the specialized programming languages in which they can most clearly express the ideas of cryptography. Tarring their descriptive and expressive computer languages as unprotected "functional" technologies and enjoining the communication of ideas because they might permit others to decrypt a copyrighted work, the court prevents cryptographers from discussing, challenging, and even developing the "technological protection measures" that will shape modern media.

[2] Quoted in Charles Petzold, *Code: The Hidden Language of Computer Hardware and Software* (1999).

Cryptography is the science of designing and analyzing secure codes and ciphers, the use of mathematical algorithms to translate plaintext messages into unreadable "ciphertext." Among cryptography's many uses are protecting the privacy of cellular telephone conversations, attorney-client correspondence, political discussions, medical records, and human rights reports, securing financial transactions, and authenticating the exchange of contractual promises, as well as controlling access to copyrighted works distributed to the public, as at issue here. Its counterpart, cryptanalysis, is the recovery of plaintext from unknown ciphertext.[3] Scientists practice the two in tandem, both developing new encryption schemes and continually "attacking" these and existing methods to test their security. Continued development of cryptography may enable the Internet to offer private communication among billions of people worldwide, and its testing is critical to enable people to trust these new means of communication.

The District Court found Section 1201 to "restrict First Amendment freedoms no more than necessary." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 327-28 (S.D.N.Y. 2000). The Section's language belies that claim, however:

[3] *See* Bruce Schneier, *Applied Cryptography*, 1-9 (2d ed. 1996). In fact, after describing algorithms in prose and mathematical formulas, Schneier includes

> 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 that effectively controls access to a work protected under this title [or] has only limited commercially significant purpose or use other than to circumvent…

17 U.S.C. § 1201(a)(2).[4]

The statute's overbroad sweep is tied to its vagueness. Since the Copyright Act protects works when they are "fixed in any tangible medium of expression," almost anything that can be encrypted may be a "work protected under this title." 17 U.S.C. §§ 102, 1201(a)(2). Likewise, the results of any cryptanalysis effort could fall within the definition of "circumvention": "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure." § 1201(a)(3)(A). Even securing the "authority" of the copyright owner of the particular work on which they are performing analysis cannot assure cryptographers that publication of their research will not be considered to "offer to the public [or] provide" a "technology, … component, or part thereof" for circumventing access or copy controls on a

pages of source code illustrating them in detail.

[4] The statute also bars technologies or devices "marketed … for use in circumventing a technological measure." 1201(a)(2)(C). The second prong, however, which captures technologies with "limited commercially significant purpose or use" other than circumvention, is of particular concern to *amici*, whose non-commercial research might be deemed to have little commercial significance.

different work encrypted by the same method. § 1201(a)(2) and (b)(1). Thuss while Congress may have aimed to protect the specific content protection systems developed by the motion picture and recording industries, its scattershot hit the entire field of cryptography. Section 1201 makes it impossible for a researcher to take apart an existing system and learn from the mistakes of the people who designed it.

Not only will they be prevented from testing the strength of existing cryptosystems, cryptographers will be hamstrung when publishing mathematics that might also be used to cryptographically protect copyrighted material. A single copyright owner may adopt a useful algorithm to protect its intellectual property, and thereby shut down the very process by which that useful algorithm was developed. No further publications about that algorithm are permitted because the author may be providing information (a "component") that will break the protection. "Primar[y] design[]" or intent is insufficient safeguard to those whose study and speech will be chilled by these provisions. Section 1201 is impermissibly vague because it "fail[s] to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999).[5]

This vagueness, if the District Court's opinion is allowed to stand, will chill researchers from publishing the results of all manner of encryption research, greatly diminishing the exchange of ideas in the field. "If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest." *Sable Communications of California., Inc. v. F.C.C.*, 492 U.S. 115, 126 (1989). Neither the District Court nor Congress could determine that a blanket ban on publishing cryptanalytic research was necessary or justifiable to protect the interests of copyright owners. Experience suggests just the opposite – that copyright owners will benefit from the stronger encryption systems developed in a climate of open inquiry.

II. Code Is Expressive Speech

Programming languages are specialized languages for the discussion of programming topics. They may express nearly all, if not all the range of human

[5] Although cryptographers may be unlikely to meet the willfulness and "commercial gain" requirements for criminal liability under Section 1204, the possibility of criminal penalties heightens the import of vagueness concerns and further chills speech and research activity.

ideas. The author of one seminal programming treatise invented an idealized machine language in which to write example programs because "a formal, precise language is … necessary to specify any computer algorithm." 1 Donald E. Knuth, *The Art of Computer Programming*, viii (3d ed. 1997). These programs were expressive even before simulators were built capable of running their code, and remain so after they may be made to "function." The expression is not only in the comments in source code, perhaps explicit notes to fellow programmers, but in the structure and operational aspects of the program itself, source or object. Whether or not they are ever input into a computer with the proper hardware and platform, code statements have the capacity to convey information to a reader who understands their language.

Code's "functional" precision gives it expressive power because its vocabulary has been built specifically for application to the types of mathematical investigations cryptographers tackle. Just as medical terminology allows doctors to communicate with the precision required to ensure correct diagnosis and treatment, the same precision that allows a compiler to translate source code to object code or a computer processor to read instructions from object code is critical to cryptographers. This language enables them to speak with clarity about the differences between a secure encryption algorithm and a similar one that is easily defeated, or to teach why one function may execute more quickly than another.

For this reason, computer programming books and computing journals have contained full or partial computer programs for many years—indeed entire libraries are filled with such books and journals.

As the Ninth Circuit recognized,

> [T]he chief task for cryptographers is the development of secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. This has the added benefit of facilitating peer review ? by compiling the source code, a cryptographer can create a working model subject to rigorous security tests. The need for precisely articulated hypotheses and formal empirical testing, of course, is not unique to the science of cryptography; it appears, however, that in this field, source code is the preferred means to these ends.

Bernstein v. Dep't of Justice, 176 F.3d 1132, 1141 *reh'g en banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).[6] Forcing cryptographers to abandon this language would be like mandating that

[6] The Opinion was withdrawn pending en banc review. After the Administration changed significantly the regulations applicable to the code in that case, the review was mooted. We do not normally cite to withdrawn opinions, but note that the court below thought *Bernstein* worthy of mention. 111 F.Supp.2d at 327 n.186.

scholars of religion never use Latin or Greek, Hebrew or Arabic, whatever the loss of nuance and inadequacies of translation.

The science of cryptography depends on cryptographers' ability to exchange ideas in code, to test and refine those ideas, and to challenge them with their own code. By communicating with other researchers and testing each others' work, cryptographers can improve the technologies they work with, discard those that fail, and gain confidence in technologies that have withstood repeated testing. The scientific method depends on experimentation and reporting of results. Just as researchers, and the Food and Drug Administration, ask to see a biologist's descriptions of the experimental setup, methodology, and intermediate results before evaluating his claims, cryptographers must review the code itself, proving its strength by tests and counterexamples.

The District Court seems at first to understand this. The court concludes up-front that "[c]omputer code is expressive," and that "it is a matter of First Amendment concern." *Universal,* 111 F. Supp. 2d at 304. The opinion thereafter runs roughshod over those concerns, however, comparing code's expression to that of a political assassination and its dissemination to the outbreak of an epidemic. *Id.* at 304, 332. While finding that "each form [human language, source code, and object code] expresses the same idea, albeit in different ways," the District Court concludes that the government may legitimately regulate any and all of these forms because of their "functionality." *Id.*, at 326, 329. Indeed, the court suggests that if asked, it would clear the field, enjoining even a description in layman's English: "the injunction drew that line [between source code and English description] only because that was the limit of the relief plaintiffs sought." *Id.* at 345n.275.

The Court's ill-defined "functionality" is both an incorrect description of the nature of computer source code and an improper restriction on speech. In this reading, Section 1201 is both overbroad and unconstitutionally vague. "[T]he very existence of some broadly written laws has the potential to chill the expressive activity of others not before the court." *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 129 (1992)

A. The O'Brien Standard Is Inappropriate

After correctly finding that both source and object code are speech, the court proceeded to pigeonhole them so narrowly as to accord them none of the First Amendment protections speech demands. Its primary error is allowing the vague characterization of code as "functional" to override its expressive properties. Such a construction is inconsistent with extensive expert testimony at trial,[7] rulings of the Sixth and Ninth Circuits,[8] and the status of software as a "literary work" protectable by copyright.[9] The court's reading of Section 1201 serves neither the ends of copyright nor those of its speakers and listeners.

The court aligns code with the expressive conduct of *O'Brien* to find the restriction of speech in Section 1201 a mere incident to the prohibition on circumvention devices. *United States v. O'Brien*, 391 U.S. 367 (1968). As described above, however, we are not speaking of "the presence of expression in some broader mosaic," but of pure expression. *Universal*, 111 F.Supp. 2d 328 n.192. Code-speech cannot be suppressed merely because it is effective at conveying ideas.

The District Court appears to condemn DeCSS because its instructions are sufficient to enable even "technologically unsophisticated persons" to descramble

[7] *See* numerous supporting declarations and trial testimony of Andrew Appel, Frank Andrew Stevenson, and David S. Touretzky

[8] *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000)("the fact that a medium of expression has a functional capacity should not preclude constitutional protection."); *Bernstein v. Dep't of Justice*, 176 F.3d 1132, 1141-42, *reh'g en banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999);

[9] 17 U.S.C. §§ 101, 117.

CSS. *Universal*, 111 F.Supp.2d at 324. Yet in no other context does speech lose its protection when it becomes more expressive. "[U]rgent, important, and effective speech can be no less protected than impotent speech, lest the right to speak be relegated to those instances when it is least needed." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 345 (1995).

Nor, as even the court recognizes, does DeCSS execute itself, but must be "downloaded and executed" by a person receiving the speech before any decryption occurs. *Universal*, 111 F.Supp.2d at 313. As posted on the website, the code was not circumventing CSS, nor could it be executed on the website to circumvent CSS. Instead, the program provided a detailed description of the reversal of the CSS process and the information to support the assertion that it would now be feasible to write a GNU/Linux DVD player. DeCSS is an explication of the CSS cipher, a description of that encryption technology that communicates a means of descrambling it. That it may be employed to decrypt files from a DVD is evidence that it is a factually accurate description.

These facts demonstrate that preventing publication of DeCSS places a content-based restriction on speech. The court necessarily looks to the expression within a computer program to determine whether its information could be used to "circumvent." Another program, "deCSS," offered for the modification of Web pages, raises no objections because it does not speak about encryption. The court, in calling 1201 a content-neutral restriction "on the nonspeech elements of expressive conduct," makes a subtle but impermissible shift in focus from the speaker to his audience. The "conduct" if such there is, is on the part of those who choose to execute DeCSS. It is as if O'Brien were prosecuted not for burning his draft card, but for giving an impassioned speech after which listeners burned theirs. Yet such speech would plainly be protected absent the highly unlikely finding of imminent incitement. The Supreme court has made clear that speech does not become "offensive conduct" because listeners may take offense. *Cohen v. California*, 403 U.S. 15 (1971). The district court imposes a heckler's veto on the assumption that some of *2600 Magazine*'s public audience 'can't handle the truth' without being incited to take illegal action.

If that is "function," then every effective piece of persuasive literature is functional — the revolutionary manifesto, the political advertisement, the lawyer's closing argument — as are the instructions to build a nuclear bomb, avoid conscription, or bake a cake. The same rationale would ban a music score or player piano roll for its function in producing music. Like these, computer code is the best means for communicating the ideas of cryptographic research. By banning forms of speech, Section 1201 suppresses content. Government cannot restrict modes of expression "without also running a substantial risk of suppressing ideas in the process." *Cohen*, 403 U.S. at 26. Such a posture is out of step with the "public interest, secured by the Constitution, in the dissemination of truth." *Garrison v. Louisiana*, 379 U.S. 64, 73 (1964).

Even the contention that code may be translated almost instantaneously into action does not strengthen the case for its suppression. "The Supreme Court has rejected the position that speech must be 'effectively answerable' to be protected by the Constitution." *American Booksellers Ass'n v. Hudnut*, 771 F.2d 323 (7th Cir. 1985) *aff'd mem.* 475 U.S. 1001 (1986).

B. Section 1201 Fails Even O'Brien's Intermediate Scrutiny

O'Brien and its progeny do not countenance suppression of pure speech as merely incidental:

> > 'A government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.
>
> [T]his passage does not foreclose consideration of First Amendment claims in those rare instances when an "incidental" restriction upon expression, imposed by a regulation which furthers an "important or substantial" governmental interest and satisfies the Court's other criteria, in practice has the effect of entirely preventing a "speaker" from reaching a significant audience with whom he could not otherwise lawfully communicate.

O'Brien, 391 U.S. 388-89 (Harlan, J., concurring)

Moreover, *Reno v. ACLU* instructs that we may not limit communication on the Internet to that fit for a sandbox, nor prohibit communications there because alternate channels exist. *Reno v. ACLU*, 521 U.S. at 880. Rather, "the Internet 'is a unique and wholly new medium of worldwide human communication.'" *Id.* at 850, (quoting *ACLU v. Reno*, 929 F.Supp. 824, 844 (E.D. Pa. 1996)). The district court turns this analysis on its head, never searching for adequate alternatives yet contending that because code-speech will necessarily appear on the Internet, that medium's broad dissemination justifies holding its content to the lowest common denominator. "Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used." *Universal*, 111 F.Supp. 2d at 331. Suddenly, because a speaker can reach a large and diverse audience, he is responsible for the actions of every one of its members? The court reduces the scientific community's discourse to the level fit for presumed movie pirates. *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 134 (1992) ("Listeners' reaction to speech is not a content-neutral basis for regulation").

Nor can the effective suppression of code-speech be dismissed as a mere "secondary effect" of legitimate congressional purpose of suppressing copyright infringement. *Universal*, 111 F.Supp.2d at 329. Like the Communications

Decency Act struck down in *Reno v. ACLU*, Section 1201 is aimed at the "primary effects of … speech, rather than any 'secondary' effect of such speech … and as such, cannot be 'properly analyzed as a form of time, place, and manner regulation.'" *Reno*, 521 U.S. 844, 868 (1997) (quoting *Renton v. Playtime Theaters, Inc.*, 475 U.S. 41, 46 (1986)). As viewed by the district court, the most dangerous feature of DeCSS is the knowledge it conveys of the weaknesses of the CSS scheme. Section 1201 therefore aims to prevent the "viral" spread of knowledge in order to shore up the "technological protection measure" it describes.

The argument for content neutrality thus fails on two independent grounds. First, unlike the *Renton* zoning ordinance, the District Court's Section 1201 leaves *no* room for code-speech about decryption. Section 1201 is not a time, place, or manner restriction. Rather, if applied to computer code, it is targeted directly at the ideas expressed in that code and restricts publication of them at all times, in all places and in all manner. "The First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic." *Consolidated Edison v. Public Service Commission*, 447 U.S. 530, 537 (1980). Second, the "effect" the court takes aim at is a *primary* effect of the speech — understanding of the weakness of the CSS algorithm. The "function" Kaplan ascribes to DeCSS, that of giving precise, easily followed instructions for the descrambling of CSS, is inseparable from the expression of detailed information about the CSS algorithm and its reversal, and listeners acting on that knowledge. "Listeners' reactions to speech are not the type of 'secondary effects' we referred to in *Renton.*" *Boos v. Barry*, 485 U.S. 312, 321 (1988).

The District Court adds yet another attack on speech if its distinction between impermissible "offering" and permitted commentary is the intent to convey a message. *Universal*, 111 F.Supp.2d at 341 (barring linking to websites "for the purpose of disseminating [the DeCSS] technology"). By targeting purposeful speech, "this reasoning turns the First Amendment on its head." *Foti v. City of Menlo Park*, 146 F.3d 629, 639 (9th Cir. 1998) (invalidating ban on signs on parked cars "designed to function as a billboard" that permitted signs with no such design.) "Government can assert no substantial interest in suppressing speech when the speaker intends to communicate but permitting the same speech if incidental to another activity." *Id.*

Finally, the statute is underinclusive, establishing an arbitrary distinction between those with the skill to conduct reverse engineering and those without. "Reverse engineers," "encryption researchers" and "security testers" are permitted to speak, among themselves at least, while those who cannot conduct reverse engineering themselves are barred from the opportunity to learn from the work of others and prohibited from discussing the technologies thus discovered. If these over-narrow exceptions prevent a journalist from sharing with the public the legitimately obtained truthful information his sources provide, they cut off not only the press freedom to speak, but the public's right to learn. "It is now well established that the Constitution protects the right to receive information and ideas." *Stanley v. Georgia*, 394 U.S. 557, 564 (1969), *citing Martin v. City of Struthers*, 319 U.S. 141, 143 (1943)("This freedom [of speech and press] ... necessarily protects the right to receive"); *Lamont v. Postmaster General*, 381 U.S. 301, 307-08 (1965) (Brennan, J., concurring).

III. The Encryption Research Exemption Is Insufficient

Amici are not comforted by the encryption research exception of § 1201(g). While the exception was apparently intended to exempt cryptographic research from the prohibitions of the anticircumvention rule, it is so parsimonious as to be of little practical value. Its content- and status-based exemptions from the general prohibition further highlight the infirmities of the entire Section. Moreover, 1201(g)'s conditions impermissibly place a prior self-identification and licensing requirement on would-be researchers.

Subsection (g) exempts some encryption research from the broad prohibition of Section 1201. To earn the exemption, researchers must first make "a good faith effort to obtain authorization before the circumvention." § 1201(g)(2)(C). Even after such prior licensing application, their research will be evaluated against several "factors":

> (A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;
>
> (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and
>
> (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

1201(g)(3). The subsection offers limited permission for a researcher to develop "technological means for research activities" and to "provide the technological means to another person with whom he or she is working collaboratively." 1201(g)(4).

The exception of 1201(g) endorses a fundamentally mistaken conception of cryptographic science, one in which advances are predictable, generated only from within an "establishment," and where limited, strictly regulated testing suffices to assure the security of cryptosystems. Thus the cryptographer must be prepared to satisfy a court that his work is aimed at "advancing the state of knowledge in the field" or "assisting in the development of encryption products." No leeway is given to the student who repeats a tried experiment as a step in his own education that does not yet advance the state of knowledge, nor to the experimenter not yet prepared to demonstrate the "assistance" her tests provide.

Cryptography is not a "members only" club. Anyone with the motivation to learn and ability to contribute has the right to do so.[10] The factors a court is instructed to "consider[]" in determining whether a person qualifies for an exemption not only discriminate based on status irrelevant to cryptographic science, but close the science to newcomers. *Amici* do not delineate their field by "course of study" or "employ[ment]" so much as by the quality of the participants' contribution.[11] Albert Einstein began to develop his theory of relativity while a Swiss patent office clerk.

[10] *See, e.g.,* Bruce Schneier, *Self-Study Course in Block Cipher Cryptanalysis,* Cryptologia, v.24, no. 1, Jan 2000, pp. 18-34, <http://www.counterpane.com/cryptanalysis.pdf> (visited January 24, 2001). "The only way to learn cryptanalysis is through practice. A student simply has to break algorithm after algorithm, inventing new techniques and modifying existing ones. Reading others' cryptanalysis results helps, but there is no substitute for experience."

[11] Even the Federal government does not make status-based judgments when searching for encryption standards, but opened its search for an Advanced Encryption Standard to "the public, academic/research communities, manufacturers, voluntary standards organizations and Federal, state, and local

Yet 1201(g) is not merely bad science but bad law. Equal protection concerns forbid favoring one group over another in regulating speech. *See Carey v. Brown*, 447 U.S. 455, 459-471 (1980); *Police Dept. of Chicago v. Mosley*, 408 U.S. 92, 98-102 (1972). Moreover, even this limited class is given permission to express only certain favored viewpoints.

The District Court's test clearly expresses preference for discussions of the strengths of an encryption technology over those describing its weaknesses: participants in the former may use code or any other language, the latter must hedge their discussion in abstractions, avoid linking to their colleagues' websites, and by no means make such statements as "Stop the MPAA." *Universal*, 111 F.Supp.2d at 341, 312-13. Yet this viewpoint preference fails to achieve its ostensible purpose, as explorations of encryption's vulnerabilities are as important to strengthening the protection it offers as abstract discussions of its strengths. Detailed analyses point out immediate problems to be fixed and future pitfalls to

government organizations." *See* 62 Fed. Reg. 48051-48058 (1997) <http://csrc.nist.gov/encryption/aes/pre-round1/aes_9709.htm> (visited January 25, 2001). It subsequently evaluated the submissions in part by opening them to public comment and cryptanalysis. "Since security will be the most important characteristic of the selected algorithm(s), NIST strongly encourages and welcomes cryptanalysis of the finalists," *i.e.*, attempts to break the ciphers or descramble their output. 64 Fed. Reg. 50058-50061 (1999) avoid. The District Court impermissibly takes a side in the public debate, blocking the market for information and ideas from reaching a conclusion based on reasoned analyses and scientific exploration.

The narrow exemption fails to recognize the interconnection of cryptanalytic testing with security: What look to the layperson like attempts at "circumvention" are key to evaluation and strengthening of encryption technologies. While anyone can create an algorithm that he himself cannot break, only an experienced cryptanalyst can design a *good* algorithm – with experience gained from analysis of other people's ciphers. Moreover, we cannot prove a technology secure, only demonstrate that no known attack has succeed against it in a given timeframe.

Thus only in an open environment, where cryptographers – and not only "collaborators" in developing the technology who have a stake in its seeming security – can perform tests in a peer review of encryption technologies, can cryptographers or the public place trust in those that pass the review. While the District Court likens publication of DeCSS to dissemination of the combination to a bank's safe, is the bank more secure if its lock succumbs to the first visitor who twiddles the knob to zero, despite that combination's never being published?

<http://csrc.nist.gov/encryption/aes/round2/aes_9909.htm> (visited January 25, 2001).

Cryptographic research can steer users of encryption, including publishers, away from such weak locks.

The District Court deemed defendants' publication of DeCSS ineligible for the "encryption research" exception of 1201(g) because "[t]hey posted DeCSS for all the world to see, made no efforts to obtain authorization, and failed to provide the results of their work to the copyright owners." *Universal*, 111 F.Supp.2d 294, 321. Yet the essence of peer review is sharing research findings with "outsiders" for evaluation by those who have not been involved in the research development. As the District Court read it, Section 1201(g) does not countenance such far-flung cooperation as the Internet makes possible under its narrow "collaboration" allowance.

To obtain even this narrow exemption, a cryptographer is required to make "a good faith effort to obtain authorization before the circumvention." § 1201(g)(2)(C). First, in the context of publishing decryption code, a cryptographer simply cannot know which potential works will be decrypted by the recipients and so cannot know whom to ask.[12] Aside from the difficulty of

[12] Although 1201 is drafted to protect the rights of copyright owners, the copyright owners at trial below disclaimed the ability to authorize circumvention; the entity licensing the encryption scheme would just as likely turn the demand back to the multiple copyright owners who might be using its method. The

determining to whom he must apply, the researcher may be deterred or chilled by the requirement, both a prior licensing and a compulsion to speak. Mandating such a request, even when the immunity of Section 1201(g)(2) is not premised on the success of the "good faith effort," chills the investigation. The researcher may rightly fear denial of future access if he appraises the technology unfavorably.[13] "The First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what not to say." *Riley v National Federation of the Blind*, 487 U.S. 781 (1988).

The advancement of the science of cryptography depends on researchers' ability to study signals "in the wild," not only those codes developed for academic

copyright owner on the specific work one is decrypting may be but one of hundreds or thousands to use the same protective measure. Thus Dean Marks testified at trial that the studios could not authorize decryption.

[13] Government-imposed discretionary licensing as a condition on speech are clearly unconstitutional, because the neutrality of standards cannot be assured and because the would-be-licensee may feel a self-censorship even before application to the authorities. *See Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750 (1988); *Shuttlesworth v. Birmingham*, 394 U.S. 147, 150-151 (1969) "[A] law subjecting the exercise of First Amendment freedoms to the prior restraint of a license, without narrow, objective, and definite standards to guide the licensing authority, is unconstitutional." Nor is it more acceptable that private parties, the "copyright owners" whose works are "technologically protected," rather than the government asserts the licensing power. The government may not delegate to private actors a power it does not possess. *See Larkin v. Grendel's Den, Inc.* 459 U.S. 116 (1982).

purposes, since the implementation may be as important as the algorithm in determining a system's security. Researchers must be able to review these technologies as they find them to learn from problems in previous implementations. A requirement that they ask permission first, and the likelihood that such permission would be conditioned on their promise not to disclose the results, stunts the field's development. The principles of security and cryptanalysis must be discovered and shared, not legislated, and the Constitution assures this will be the case by protecting highly technical discourse on scientific subjects.

The Supreme Court has instructed that the "choice, between the dangers of suppressing information, and the dangers of its misuse if it is freely available, [is one] that the First Amendment makes for us." *Virginia Pharmacy Board v. Virginia Citizens Consumer Council,* 425 U.S. 748, 769 (1976) Government may not base its suppression of speech on the supposed benefits of keeping the public in ignorance, neither of the comparative price of drugs nor the weakness of the CSS cipher.

Finally, even when a researcher has made his or her way into the pigeonhole of 1201(g), its exemption does not cover all the potential liabilities under the Section. It provides no safe harbor from allegations that code that permissibly grants access is nonetheless a device that unlawfully "circumvent[s] protection afforded by a technological measure that effectively protects a right of a copyright owner" under § 1201(b)(1).[14]

That these are "factors to be considered," rather than firm requirements, does not make them less objectionable. "When the purpose and design of a statute is to regulate speech by reason of its content, special consideration or latitude is not accorded to the Government merely because the law can somehow be described as a burden rather than outright suppression." *United States v. Playboy Entertainment Group, Inc*,.529 U.S. 803 __, 120 S.Ct. 1878, 1893, (2000)

IV. Section 1201 Can Be Read to Be Compatible With the First Amendment

The Digital Millennium Copyright Act twice disclaims its intent to regulate speech, in sections the district court appears to ignore. Thus 1201(c)(4) states that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products," and 1203(b)(1) instructs that a court "in no event shall impose a prior restraint on free speech or the press protected under the 1st amendment to the

[14] Again, since the anti-trafficking provisions do not require proof of any actual infringement, it is irrelevant in a 1201(b) action that none of the researcher's colleagues uses the provided code to infringe a copyright. As do plaintiffs below, a plaintiff may simply allege that non-conformant access facilitates copying or the creation of an unauthorized derivative work.

Constitution." Without these safeguards in place, the DMCA imposes an impermissible burden on cryptographers' freedom of expression.

Fortunately, the statute can be read to be constitutional if we take into account 1201(c)(4), which the court inexplicably ignores. The plain import of this subsection is to exclude speech from the description of "technology, product, service, device, component, or part thereof," even when that speech takes the form of specialized languages of computer code. *See Meyer v. State of Nebraska*, 262 U.S. 390 (1923) (overturning state law conviction for the teaching of German). DeCSS code is therefore not a "technology" whose "trafficking" can be regulated, but speech itself, whether communicated in private between researchers at an academic institution or over the Internet among programmers who meet through their common interest in playing DVDs on alternate platforms.

With the enactment of Section 1201, code is quite literally made law – the technological measures copyright owners impose on media set the limits on what viewers may lawfully do with copyrighted works. When these technological measures involve encryption, we rely on cryptographers to read this law and assure that it does not overstep its limits. The provisions of the DMCA must not be permitted to hide the terms of engagement.

CONCLUSION

For the foregoing reasons, the decision below should be reversed.

Respectfully submitted,

JENNIFER STISA GRANICK, ESQ.
California State Bar Number 168423
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-0014

Counsel for *Amici Curiae*

Date: January 26, 2001