Ethics and Information Technology **3:** 21–33, 2001.

Code as speech: A discussion of *Bernstein* v. *USDOJ*, *Karn* v. *USDOS*, and *Junger* v. *Daley* in light of the U.S. Supreme Court's recent shift to Federalism

Jean Camp[1] and K. Lewis[2]
[1]*Kennedy School of Government, Harvard University, Cambridge, MA 02138 (E-mail: Jean_camp@harvard.edu);* [2]*Graduate School of Industrial Administration, Carnegie Mellon University, Pittsburgh, PA 15213 (E-mail: kdl69@msn.com)*

Abstract. The purpose of this paper is to address the question of whether computer source code is speech protected by the First Amendment to the United States Constitution or whether it is merely functional, a "machine", designed to fulfill a set task and therefore bereft of protection. The answer to this question is a complex one. Unlike all other forms of "speech" computer source code holds a unique place in the law: it can be copyrighted, like a book and it can be patented like a machine or process.[1] Case law, intellectual property law and encryption export regulations all reflect this contradictory dichotomy.

Key words: artistic license, BSD, code, cryptography policy, democracy, encryption, free software, governance, GPL, intellectual property, law, liability, open source, source code, speech, UCITA

Introduction

There are currently three cases before three separate federal courts that address as their core issue whether code is speech. The three cases are *Bernstein* v. *US Dept. of Justice*,[2] *Junger* v. *Daley*[3] and *Karn* v. *US Dept. of State*.[4] Both a Federal District court and a Federal Appeals court have heard each of the three cases. To date the courts have been split with Bernstein having initially won First Amendment protection for his code in the Ninth Circuit Court of Appeals before being remanded for an en banc rehearing; *Junger* having won First Amendment protection for his code and been granted a remand back to the lower court for rehearing after winning his appeal before the Sixth Circuit Court of Appeals; and Karn having been remanded back to the lower court for rehearing due to a change in the law The core causes of action in all three cases are similar enough in general: the plaintiffs, *Bernstein*, *Karn*, and *Junger*, all seek to have the current Federal regulations that governs the exportation of encryption software declared unconstitutional for violating the First Amendment.

In each case the plaintiff sought to export encryption source code in digital form; in each case the export was deemed covered by federal regulations and therefore each plaintiff was faced with the choice of either registering with the government and acquiring a license or not going forward with the export. The facts in *Bernstein* and *Junger* are almost identical. Both Bernstein and Junger are university Professors who seek to publish encryption software used in their respective classes on their universities' web site in attempts to educate their students and foster better understanding of encryption software. It is interesting to note that while Bernstein and Junger share a passion for encryption software, they arrived at their shared interest from very different backgrounds. Bernstein is a Doctor of Philosophy in mathematics who looks at encryption from the standpoint of the mathematics that is the core of encryption; Junger is a Doctor of Law who looks at encryption from the standpoint of policy seeking to explore the interface of law, technology, and public policy. Bernstein, a mathematician, is a Professor of mathematics, statistics, and computer science at the University of Illinois. Junger, an attorney, is a Professor of law at Case Western Reserve University Law School. This difference of background is not essential to either parties argument but does help bolster the contention shared by each plaintiff that computer code is speech and that computer languages are languages used to communicate complex ideas.

It is important to note that we are addressing the singular issue of whether computer source code is speech protected by the First Amendment and not the several other issues that were raised by the plaintiffs including violations of the Fourth Amendment and the

[1] Camp and Syme, *The Governance of Code: Code As Product, Service and Speech*, Ethicomp 2001, submitted.

[2] *Bernstein* v. *US Department of Justice*, 97-16686, 4222, (Ninth Circuit Court of Appeals (1999)).

[3] *Junger* v. *Daley*, No 96-CV-1723 (N.D. Ohio, July 2, 1998).

[4] *Karn* v. *United States Dep't of State*, 920 F. Supp. 1, 9 n. 19 (D. D.C. 1996).

separation of powers clause of the U.S. Constitution. It is our belief that computer languages are languages used by individuals from varied backgrounds to communicate sophisticated ideas that cannot truly be conveyed in any other manner and that such communication is speech protected by the First Amendment. We share[5] the contention that the Federal Government's current manner of preventing the export of strong encryption is an attempt to restrict the US Citizens' access to strong encryption technology and that this attempt is a violation of the right to freedom of speech guaranteed by the First Amendment to the U.S. Constitution. A foundation of our argument is that source code is speech.

Notice we make only this claim of source code, not of any other forms. Computer software written in higher level languages can take two forms: source code and object code. Source code is the human readable form of a program before it has been compiled (the process of turning the source code into object code). Object code is the binary or computer readable version of the same program after being compiled – object code is not human-readable.

Cryptography, the science and practice of using encryption, and ciphers have been an element of American political life since before the country was founded.[6,7] In fact, we as citizens owe at least a small debt to the science of encryption for the birth of our nation. From the Revolutionary War to WWII encryption code has been critical for our nation, and such a role has been used to argue both for and against cryptography.

A brief history of controls on the export of encryption

In this section we give a brief background on the International Traffic in Arms Regulations (ITAR) and subsequent Export Administration Regulations (EAR) on encryption. In addition to discussing the regulations we address the Presidential Memorandum and Order that led to the shift of regulatory authority from the Department of State to the Department of Commerce. The specific language of President Clinton's order and the Department of Commerce's actions taken under the authority of that Order are illuminating and provide an interesting look at the reasoning behind the Federal Government's attempt to restrict encryption. This section consists primarily of exact definitions of otherwise general phrases, such as technical data, which are at the core of the conflict about what can and can not be encrypted.

The Arms Export Control Act (AECA) authorizes the President to control the import and export of defense articles and defense services by placing such items on the United States Munitions List (USML) [22 U.S.C. Section 2778(a)(1)] Once on the USML, and unless otherwise exempted, a defense article or service requires a license before it can be imported or exported [22 U.S.C. Section 2778(b)(2)]. The Munitions List consist primarily of weaponry, and is not generally intended for technology which has significant non-military use.

The International Traffic in Arms Regulation (ITAR) [22 C.F.R. Sections 120–30] were promulgated by the Secretary of State, who was authorized by executive order to implement the AECA. The ITAR are the regulatory controls enabled by the Act. The ITAR are administered primarily within the Department of State by the Director of the Office of Defense Trade Controls (ODTC), Bureau of Politico-Military Affairs. The regulations allow for a "commodity jurisdiction procedure" by which the Defense Department determines if an article or service is covered by the USML when doubt exists about an item [22 C.F.R. Section 120.4(a)]. The licensing requirements for defense articles and technical data are also covered by the ITAR [22 C.F.R. Section 123 and 22 C.F.R. Section 125].

Categories of items covered by the USML are enumerated at 22 C.F.R. Section 121.1. Category XIII, Auxiliary Military Equipment, includes "Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems ..." [22 C.F.R. Section 121 XIII(b)(1)]. A number of applications of cryptography are excluded particularly those that are used only to protect financial information, such as those used in automated teller machines, and certain mass-market software products that use encryption [22 C.F.R. Section 121 XIII(b)(1)].

A "defense article" is defined by the ITAR as any item or technical data that has been designated in the USML 22 C.F.R. Section 120.6. A "defense service" is any assistance rendered to a foreign person in the United States or abroad in the development or use of a defense article [22 C.F.R. Section 120.9(a)(1)] or the furnishing of technical data to a foreign person [22

[5] A. Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution", 143 *U. Penn. L. Rev.* 709, 1995. http://www.law.miami.edu/~froomkin/articles/clipper.htm

[6] D. Kahn, *The Codebreakers*. Scribner, NY, NY, 1996.

[7] John A. Frasier III, "The Use of Encrypted, Coded and Secret Communications is an 'Ancient Liberty' Protected by the United States Constitution", *Virginia Journal of Law and Technology*, Fall 1997. Section IIIA.

C.F.R. Section 9(a)(2)]. "Technical data" is defined separately and in relation to defense articles [22 C.F.R. Section 120.10] in the ITAR but it is also defined only as a defense article when it is covered by the USML [22 C.F.R. Section 120.6].

Technical data is generally information "which is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles" [22 C.F.R. Section 120.10]. It also encompasses software directly related to defense articles. Software "includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test operation, diagnosis and repair" [22 C.F.R. Section 121.8(f)]. A person who wants to export software that is not designated on the USML can apply for a technical data license. The definition of technical data includes some noteworthy exemptions. Technical data "does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain ..." [22 C.F.R. Section 120.10(a)(5)]. The public domain exemption excludes from technical data information which is "published and generally accessible" to the public through newsstands, bookstores, subscriptions, libraries, conferences and trade exhibitions [22 C.F.R. Section 120.11(a)(1)–(6)]. (Notice that while more than one of these applies to the cases at hand, the concentration in this work is on the argument that code is speech, not that the cases at hand meet particular exemptions.)

Finally, "export" is defined as "[s]ending or taking a defense article out of the United States in any manner" and as "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad" [22 C.F.R. Section 120.17].

Based on the public domain exception of the ITAR it would seem that at least Karn, if not Bernstein and Junger, could have exported his encryption source code. The code that Karn wished to export was a verbatim version of code available in a text entitled Applied Cryptography.[8] One would expect that it would have been accorded the same protection that the book itself enjoyed. While both Bernstein and Junger could arguably have been accorded the public domain protection contained in the ITAR they would surely have been able to take advantage of the ITAR research exception. Bernstein wrote his Snuffle program as part of his research carried on while working towards his Doctorate. Junger wrote his encryption programs for use in his courses on computers and the law.

The ITAR were drafted immediately following the Second World War and served as guidelines for over 40 years. By the end of the 20th Century the importance of encryption in the commercial arena was clear, and therefore President Clinton issued his Memorandum and Executive Order 13026 on November 15, 1996. This order shifted control of certain commercial grade encryption items from the Department of State under the ITAR to the Department of Commerce under the Export Administration Regulations (EAR) [61 F.R. 251]. The President states in his Executive Order his reason for continuing to exercise control over encryption software:

> I have determined that the export of encryption products described in this section could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States, and that facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm the United States national security and foreign policy interests. [Executive Order 13026, 61 F.R. 224 page 5]

This shift in regulatory authority was met with approval by many of the privacy rights groups, and was widely applauded by the commercial sector. It was regarded not only as a precursor to further relaxation of the Federal government's restrictions, but also as an immediate solution to the business problem of dealing with the Department of Defense. As a side effect, it switched the regulatory authority from one Federal department to another and also addressed a weakness in the government's argument in the trial court.

Karn's appeal before the US District Court of Appeals for Columbia was arguably poised on the brink of victory following the success of *Bernstein*; although the ruling of the California district court upon the DC District court was merely persuasive. The government, having sustained a significant loss already, could not allow a loss in the Karn case. The timing of the Executive Order meant that the DC District Court would not hear the case.

In December of 1996 the Department of Commerce (USDOC), through the Bureau of Export Administration (BXA) amended the Export Administration Regulations (EAR). Among the amended EAR provisions in question were the definition of export and the provision providing for court review of any decisions made under the regulations [15 C.F.R. Parts 734, 740].

[8] Bruce Schneier, *Applied Cryptography*. John Wiley & Sons, NY, NY, 1995.

On January 14, 2000 the Department of Commerce through the Bureau of Export Administration further revised the EAR. While these amendment specifically target encryption software and source code, the language of the amendments make it clear that the old rules are still very much in effect despite their new appearance. The amended section 742.15 "Encryption Items" reads as follows:

> Encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm national security, foreign policy and law enforcement interests. ... As the President indicated in Executive Order 13026 and in his Memorandum of November 15, 1996, export of encryption software, like export of encryption hardware, is controlled because of this functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export may convey to others abroad. For this reason, export controls on encryption software are distinguished from controls on other software regulated under the EAR.

This language makes it clear that the government continued to view encryption software as a threat to national security and that control may be exerted over such software regardless of any educational or theoretical value. The amended regulations addressed the needs of business by allowing commercial distribution for several classes of software including: any encryption to US subsidiaries; finance-specific products; encryption software including symmetric algorithms employing key lengths of 64 bits or less; and retail products when exported to individual consumers [15 C.F.R. Sec. 740.17]. However, civil libertarian concerns were yet unaddressed. In particular, source code was excluded from the Limited Exception Encryption Commodities and Software [15 CFR Sec. 740.17] portion of the amendments by the language used in Sec. 740.17(g) on open cryptographic interfaces:

> (f) Open cryptographic interfaces. License Exception ENC shall not apply to exports or reexports of encryption commodities and software including components, if the encryption product provides an open cryptographic interface (as defined in part 772). This does not apply to source code that would be considered publicly available under sec. 734.3

Therefore under the draft amendments to the EAR Karn, Bernstein, and Junger would at a minimum have to submit their code for review and would in all likelihood have to receive a license as well. Since the review requirements are unconstitutional as a prior restraint of speech the legal front remained unchanged for these cases.

When Professor Bernstein asked for clarification of his position under the amended regulation he received a reply from the Director for the Office of Strategic Trade and Foreign Policy Controls indicating that he no longer needs a license. While this response is borne out of an interpretation of the amended regulations it is staved off Bernstein's request for a new trial to challenge the amended EAR.[9]

Code as speech

In this section we attempt to give public policy reasons for source code being treated as speech. The word code to a legal mind is that which details what actions are permissable in the analog world. The word code to a technical mind is that which details what actions are possible in the digital world.

Note that the words code, standards, protocol, language, and software differ as follows. Standards are documents that define protocols. Protocols are communications standards that define a series of messages and the syntax for those messages. Code is the implementation of the protocol (which should be compatible with the standard). Code is the actual software, the detailed language description of how the standard actually works in practice. Standards are the ideals of how the code should work. Code is software. Language is the way the software is written, for example Java v. C++ is not unlike French v. English.

At the trivial level, both legal code and object code are code because they are both pre-arranged sets of meanings assigned to particular symbols. Reading the law, understanding its subtleties, interaction with other laws, and legal implications requires specialized training. For example, in the computer programming language C the symbol $ is used to denote a string variable that is capable of being assigned a text value. In the language of the law the symbol § is used to denote a section of the legal code. The law is not written in casual language, despite that fact that it is written in the vernacular with only sparse use of Latin. Reading computer code also requires specialized training to understand its subtleties, interaction with other code, and social implications despite the use of vernacular language constructs.

We argue in this section that computer code, like legal code, is speech, specialized formal speech but

[9] Law Offices of McGlashan and Sarrail, *Bernstein's Brief Requesting Remand to Dist. Court*, March 3, 2000. Available at http://www.eff.org/pub/Privacy/Crypto_export/Bernstein_case/Legal/20000303_bernstein_remand_brief.html

speech nonetheless. We further argue that, like the law, it is speech critical to expanding and understanding the discourse currently raging about the structure of our increasingly information based society. We call upon the court to recognize the importance of Bernstein's ability to distribute cryptographic code specifically because the code itself is a message to the mathematicians and cryptographers who understand the language of computers, just as a proposed law is a message to the lawyers and legislators who understand the language of the law. Code distribution, adoption, and alteration is the moot court of the computer profession.

To support our argument we use both the previous analogy and the following three examples. The first example is one of speech at the network level. The second example is one of code as a means of facilitating association and trust. And the third example is one demonstrating the use of code as a method of ensuring equity.

Electronic speech on the Internet has been given protection by the courts in *Reno* v. *American Civil Liberties Union* because there was no feasible way to control and filter speech in such a manner that protected speech prohibited for children but protected for adults except on the desktop. On the Internet, content is transparent to the protocol; the network simply forwards bits. (Here we mean transparent in the engineering sense, which means "invisible," as opposed to transparent in the governance sense, meaning "visible".) There is no billing associated with content delivery at the bit level or the connection level. Contrast that with the cable television (CATV) networks. With CATV it is possible to block content at the behest of the cable provider or subscriber but it is the cable provider who ultimately determines the content received by the subscriber. In addition, while billing information is available concerning each of the channels that the viewer is offered by a particular CATV provider there is no one provider that offers all of the possible channels.

Recall that in the early nineties the CATV template was the model for the then-emerging broadband information super-highway. While the vision from the top down was of hundred of channels what has emerged from the bottom up has been a construction with millions of web pages. The Internet has been widely adopted, no doubt in part because it facilitates the devolution of content control to the user as opposed to concentrating control in the center. People were provided a choice and adopted an open TCP/IP – based system. (TCP/IP is the underlying protocol which connects the network of networks that comprise the Internet.) TCP/IP is available for all operating systems in use today – and hardware platforms – so these computers (UNIX workstations; PCs running MS-DOS, Windows, or OS/2; Apple Macintoshes, IBM Mainframes; DEC Minicomputers; etc.) can all communicate. When that choice was offered, open vs. closed system, the open system won out. Because the same wires using different protocols were adopted the information infrastructure is fundamentally different in terms of speech, democracy, and autonomy than the original broadband vision. Individuals could adopt the protocol because it was an open standard. Freeware and shareware implementations of the software necessary to connect to the Internet were available. By choosing to connect to the Internet as opposed to using the disks sent by AOL – proprietary software – people choose an open structure for the information infrastructure.

The original information super-highway vision suggested a service of hundreds of television channels with the citizen as passive viewer, only active enough to make a purchase. On the Internet, in contrast, the consumer is active: as a neighbor in chat groups, as a participant in political debates, and as an empowered consumer in Internet commerce. These fundamental differences are made possible because people can choose different protocols. The same cable wires, phone wires, and physical realities of microelectronics would have governed the 500-channel mall that was envisioned and governs the Internet that has come to be. The critical difference is that people chose the open medium where everyone has a voice. Users choose a system allowing them to communicate as well as to consume, to speak as well as to listen. Those choices are made through the selection of a network protocol. The choice of protocol was enabled by code. Without the choice of code there would have been no choice of information infrastructure. Today's Internet user, instead of chatting, posting, authoring, arguing, contributing, and buying would instead be pinned passively to the sofa by a selected set of hundreds of channels with no feedback mechanism but the button on the remote labeled "BUY". The choice of code and the freedom to offer new versions of code has played a critical part in the construction of the information infrastructure and therefore the information based society.

The anonymizer was originally a project of Justin Boyan, a Carnegie Mellon computer science student. Mr. Boyan created a proxy for anonymous Web browsing. A proxy is a piece of software that sits between a network user and the network to provide a measure of privacy by routing all network requests through a filter that masks the actual characteristics of the user to the network and yet returns the information sought by the user. He also created a script for telling each browsing person what information was

available about them – usually machine, site previously visited, and domain. Most users simply cannot see the footprints they leave across cyberspace.

Internet privacy has implications for speech, for association, and for personal privacy. Courts have found in the past that full freedom of speech and association require privacy, or at least freedom from surveillance. Invisible surveillance is surveillance nonetheless. (See *Katz* v. *United States*, 389 U.S. 347; *Bates* v. *Little Rock*, 361 U.S. 516; *NAACP* v. *Alabama*, 357 U.S. 449 for analyses of autonomy and surveillance.)

Those who install anonymous Web proxies and use identity-protecting software are using code to extend trust. The terms on which consumers and citizens extend trust on the Internet are not terms that can be negotiated in contract or face-to-face. Privacy protecting software allows individuals to opt out of the privacy bargain offered by the network service providers, the merchants, and the politicians. Exhibiting a desire for privacy while also showing a desire for the content or goods offered is a voice, a way of being heard. It is less action than other, direct actions that are speech, such as burning a draft card [*United States* v. *O'Brien*, 391 U.S. 367 (1968)] or the flag [*United States* v. *Eichman*, 496 U.S. 310 (1990)]. Privacy-protecting code prevents others from using their technical acumen to take action on information about a citizen. Using such code is a demand for autonomy, a refusal of surveillance.

Cryptography plays a critical role in choices with respect to network privacy. According to the National Academy of Science:

> [I]t is clear that the development and widespread deployment of cryptography that can be used to deny government access to information represents a challenge to the balance of power between the government and the individual. Historically, all governments under circumstances that further the common good, have asserted the right to compromise the privacy of individuals. . . . [U]nbreakable cryptography for confidentiality provides the individual with the ability to frustrate assertions of that right.[10]

The codes in question are proposed rules as certainly as the drafts of law being debated by legislators in state houses across the country.[11] Source code in essence argues for certain behaviors to be allowed or restricted in the virtual world in the same way a model law argues for a set of allowed or restricted behaviors in the physical world. In the same manner as a code of conduct argues for given practices, the code of the Internet argues for set protocols and delivery mechanisms.

As with these others codes only some empowered individuals can embrace the given codes. Only gardeners can grow their own organic produce; only the infogensia can install strong cryptography. Yet the ability to offer these standards in the larger market of ideas (and practice) is a critical element of discourse. Adoptions may lead to change, in the same way in which adoptions of other ideas may lead to change. Because citizenry cannot read code does not make its adoption less powerful; much of the citizenry cannot name an enlightenment philosopher but most have nonetheless integrated the ideas into their daily lives.

Without source code there is no argument, no debate about the options in constructing an information society. There is only command. Without source code there is no visible debate. There is no certainty. Blind prohibition of code that would enhance privacy has a *prima facia* chilling effect on the debate about privacy. How can one change the law without the right to read it, edit it, and offer alternatives? Without the ability to freely distribute source code there is less discourse about the future of the Internet, less philosophical debate about the nature of privacy for our electronic selves, no ability to replace even a single rule.

Cryptographic code is only the most obvious case of source code as speech. Source code in security is explicit in its goals. Cryptographic source code offers arguments about the balance of state power, corporate power, and personal autonomy. By enabling strong signatures, source code enables privacy in preventing incorrect attribution. By requiring key escrow of signature keys, individuals are placing a high level of trust in the state. Programmers should be able to prove their opinions about what is possible to the public. By offering both authentication and anonymity, strong cryptography extends the range of opinions and debates about the speech. In enabling anonymity source codes offers an argument about the proper balance between privacy rights of autonomy (requiring anonymity) to privacy rights of seclusion, which would prevent anonymous slings and arrows.

Those who believe in technological utopia have embraced the information infrastructure as extant in the Internet as the pinnacle of democracy. Modern optimists point to the availability of speech, the difficulty of censorship, the lack of hierarchy, and above all the malleability of a system built on computer code. Technophobes point to the ease of surveillance, requirements for wealth, tendency for corporate

[10] National Research Council, *Cryptography's Role in Securing the Information Society*. National Academy Press, Washington, DC, 1996.

[11] Lawrence Lessig, *Code and Other Laws of Cyberspace*. Basic Books, NY, NY, 1999.

control, and the threat of the malleability of code. Source code is complicated; source code is debate. Without code there is no discussion in the virtual world about the virtual world and without discussion and debate there can be no marketplace of idea. Source code is speech which empowers the individual against possible errors or abuses of governance at the state and Federal level.

The cases in question: Karn

We address *Karn*[12] first as he was the first to file a lawsuit and as the facts of his case, while not identical to *Bernstein*[13] and *Junger*,[14] are close enough to the other cases to provide a basis for understanding the nature of the regulations at issue.

Karn is based on a slightly different fact pattern than either Bernstein or Junger. All three cases share the similarity that each plaintiff sought to "export" source-code encryption software and each was told that they had to register as arms-dealers under the ITAR. In 1994 Phil Karn sought a ruling from the US Department of State on whether the book, Applied Cryptography,[15] and a companion floppy disk were covered by the ITAR. The central issue in Karn was the Department of State's ruling that the book itself was freely exportable from the United States while the floppy disk was not, although both the disk and the book contained identical copies of the complete source code for several strong cryptographic algorithms.

The Department of State formally designated the floppy disk as a "defense article under category XIII(b)(1) of the United States Munitions List" but declared that the book was freely exportable. More recently the disk was reclassified as a controlled "Encryption Item" (EI) and therefore still cannot be legally exported from the US. Note that the source code in the book can be typed into a computer, compiled, and used by anyone who has a familiarity with ANSI C+, a very common computer language, so by allowing the book to be exported the government has done an end run around itself in its attempts to safeguard the national security.

According to the government the book itself is clearly protected by the First Amendment yet much of the same text contained in the book, when digitized, and transferred to a media different from paper suddenly becomes merely functional and therefore suffers the loss of the First Amendment protection. Even those not versed in the intricacies of the law should be able to see that if a message is protected then transferring that message to different media does not strip it of that protection. An easy analogy is to observe that a political speech whether given in person or delivered via television or some other form of transmission would be protected under the First Amendment. Shifting the mechanism by which the speech is delivered does not strip the message of Constitutional protection.

To follow the US Government's argument, if a person is wealthy enough to publish their thoughts on encryption, including the actual language of any programs they have written, in the traditional manner of ink on paper then they can do whatever they wish with the final product including giving or selling the final product to anyone. However, if said person, were not wealthy enough to publish their thoughts in the traditional manner, but savvy enough to publish their source code on the Internet, perhaps through any number of free web publishing sites or through a school, they lose the protections extended to the first individual and risk becoming a criminal.

The US District Court for the District of Columbia's summary judgment in favor of the US Government was worded in very strong language:

> This case presents a classic example of how the courts today, particularly the federal courts, can become needlessly invoked, whether in the national interest or not, in litigation involving policy decisions made within the power of the President or another branch of the government. The plaintiff ... raises administrative law and meritless constitutional claims because he and others have not been able to persuade the Congress and the Executive Branch that the technology at issue does not endanger the national security. This is a 'political question' for the elected branches under Article I and II of the Constitution.[16]

This language makes it clear that the court was unsympathetic towards Karn and saw him as someone who was wasting the court's time.

The court applied the O'Brien test.[17] The O'Brien test requires that the government's regulations be content neutral, within the constitutional power of the

[12] *Karn* v. *United States Dep't of State*, 920 F. Supp. 1, 9 n. 19 (D. D.C. 1996).

[13] *Bernstein* v. *US Department of Justice*, 97-16686, 4222 (Ninth Circuit Court of Appeals (1999)).

[14] *Junger* v. *Daley*, No 96-CV-1723 (N.D. Ohio, July 2, 1998).

[15] Bruce Schneier, *Applied Cryptography*. John Wiley & Sons, NY, NY, 1995.

[16] *Karn* v. *US Department of State*, 95-1812 US District Court District of Columbia.

[17] *Bernstein* v. *US Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997.

government, and must further a substantial government interest. Thus the incidental restrictions on alleged First Amendment freedoms was no greater than was essential to the furtherance of that interest. Unfortunately, the O'Brien test is not the test that should have been applied in this situation. The O'Brien test is applied when the regulation is primarily to restrict action, and speech restrictions are incidental. An example application of the O'Brien test is a regulation preventing billboards from blocking a line of sight necessary for a driver to safely maneuver. A different, more stringent test, is applied when the core of the regulation is restriction of speech, for example a regulation blocking Safe Sex ads must meet this more strict Freedman test.

As the US District Court for the Northern District of California noted in the third *Bernstein* case, code is expressive and therefore, the central issue is whether the regulations act as a prior restraint on speech in violation of the First Amendment. Discussion of the District Court decision in *Bernstein* follows.

The cases in question: Bernstein

The US District Court for the Northern District of California heard three arguments from Bernstein and the federal government and handed down three separate decisions all in favor of Bernstein. The cases will be referred to here as *Bernstein* I,[18] II,[19] and III.[20]

The court in *Bernstein* I stated clearly that source code is speech "(t)he distinguishing feature of source code, is that it is meant to be read and understood by humans and that it can be used to express an idea or a method." It found that source code is the best way of describing encryption ideas, better than English prose or mathematical notation: "(b)y utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve."

To apply the O'Brien test the court would have had to have found, as the DC Court in Karn held, that code was not speech but rather merely functional and thus only granted intermediate scrutiny instead of the full protection of the First Amendment. Once the court found that code was speech this precluded the application of the O'Brien test and necessitated the test. Under the Freedman test the regulations could survive Bernstein's constitutional attack if it were found that his due process rights were respected. In 1965, the Supreme Court formulated the test under which a prior restraint might be found constitutional: (1) any restraint must be for a specified brief period of time; (2) there must be expeditious judicial review; and (3) the censor must bear the burden of going to court to suppress the speech in question and must also bear the burden of proof.

The District Court in *Bernstein* III when applying the Freedman test found that "(t)he ITAR scheme, a paradigm of standardless discretion, fails on every count. This court finds nothing in the ITAR that places even minimal limits on the discretion of the licensor and hence nothing to alleviate the danger of arbitrary or discriminatory licensing decisions."

In its ruling the court held that allowing printed source code to be exported undermined the government's claim that this export control scheme protects any national security interest. The court also noted that distinguishing print from electronic forms of communication probably violates the First Amendment under *Reno* v. *ACLU*, 76, which held that Internet speech deserves the same protections as printed speech.

In July of 1998 the US District Court for the Northern District of Ohio Eastern Division granted summary judgment for the US Government against Junger. As in Karn and Bernstein, Junger sought injunctive relieve and summary judgment on First Amendment grounds stating that the EAR was a prior restraint on speech, 77.

The court held that "the Export Regulations are constitutional because encryption source code is inherently functional, because the Export Regulations are not directed at source code's expressive elements, and because the Export Regulations do not reach academic discussions of software, or software in print form. For these reasons, the Court grants the government's motion for summary judgment and denies Junger's motion for summary judgment." As in *Karn*, this court misunderstood the nature of source code and applied the O'Brien test.

In explaining the standard that it would use in examining the issue the court stated "(i)f the Export Regulations are not expressive and if the Export Regulations are not aimed at the content of the ideas, then the Court reviews the regulations under an intermediate scrutiny standard. Under intermediate scrutiny, a law is constitutional if it furthers a substantial governmental interest, if the interest is unrelated to the suppression of free expression, and if the restriction is no greater than is essential to the furtherance of that interest." The core problem with the court's reasoning is the finding that source code is not expressive:

In reviewing governmental regulation of computer

[18] *Bernstein* v. *US Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996).

[19] *Bernstein* v. *US Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996).

[20] *Garcia* v. *San Antonio Municipal Transit Authority*, 469 U.S. 528 (1985).

> software, the Court need examine the software involved. Certain software is inherently expressive. Such expressive software contains an "exposition of ideas," *Chaplinsky* v. *State of New Hampshire*, 315 U.S. 568, 572 (1942). In contrast, other software is inherently functional. With such software, users look to the performance of tasks with scant concern for the methods employed or the software language used to control such methods . . .

Among computer software programs, encryption software is especially functional rather than expressive. Like much computer software, encryption source code is inherently functional; it is designed to enable a computer to do a designated task. Encryption source code does not merely explain a cryptographic theory or describe how the software functions. More than describing encryption, the software carries out the function of encryption. The software is essential to carry out the function of encryption. In doing this function, the encryption software is indistinguishable from dedicated computer hardware that does encryption.

In the overwhelming majority of circumstances, encryption source code is exported to transfer functions, not to communicate ideas. In exporting functioning capability, encryption source code is like other encryption devices. For the broad majority of persons receiving such source code, the value comes from the function the source code does".[21]

The court examines the *Bernstein* decision and declares that the decision in *Bernstein* was unsound. In distinguishing the *Bernstein* decision the court states, "(s)ource code is "purely functional," 922 F. Supp. at 1435, in a way that the Bernstein Court's examples of instructions, manuals, and recipes are not. Unlike instructions, a manual, or a recipe, source code actually performs the function it describes. While a recipe provides instructions to a cook, source code is a device, like embedded circuitry in a telephone, that actually does the function of encryption."

This argument that "source code is a device" is not true and shows again the court's misunderstanding of the difference between source code and object code. Source code on its own is useless much like a music score on its own is useless. However, in both cases the original message, when passed through a "compiler" is transformed into something that a machine can handle and through this transformation a second, different, product is produced. The compiler in the case of source code is another computer program which interprets each line of code and translates it into a machine readable string of 0's and 1's. The compiler in the case of a piece of sheet music is the musician who translates the notes into finger movements applied to the appropriate instrument.

The court rejects the application of the prior restraint challenge by stating, "(e)xporting encryption source code is not an activity that is "commonly associated with expression." Source code is a set of instructions to a computer that is commonly distributed for the wholly non-expressive purpose of controlling a computer's operation. . . . It may, as the Court has noted, occasionally be exported for expressive reasons. Nevertheless, the prior restraint doctrine is not implicated simply because an activity may on occasion be expressive." The court's misdefinition of source code as primarily functional and only occasionally expressive results in another misapplication of the O'Brien intermediate scrutiny test in lieu of the proper Freedman strict scrutiny test.

On May 6, 1999, the Circuit Court handed down a 2-1 decision upholding the District Court's ruling in *Bernstein* III. Judge Fletcher wrote for the majority, and articulated that, indeed, the ITAR and the EAR export restrictions against encryption are an unconstitutional prior restraint of free expression, impermissible under the First Amendment.

The court re-examined whether source code is speech and held that "cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. . . . In light of these considerations, we conclude that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine." The court continued its statement that source code is speech when it noted "the distinction between source code and object code . . . (is) that source code is not meant solely for the computer, but is rather written in a language intended also for human analysis and understanding."

In applying the prior restraint doctrine based on the Freedman test the court found that the EAR clearly failed the test: "We find that the EAR regulations (1) operate as a prepublication licensing scheme that burdens scientific expression, (2) vest boundless discretion in government officials, and (3) lack adequate procedural safeguards. Consequently, we hold that the challenged regulations constitute a prior restraint on speech that offends the First Amendment."

In its only mention of the O'Brien decision the court noted that the government's argument, when pared to its core, "suggests that even one drop of 'direct functionality' overwhelms any constitutional protection that expression might otherwise enjoy. This

[21] John A. Frasier III, "The Use of Encrypted, Coded and Secret Communications is an 'Ancient Liberty' Protected by the United States Constitution", *Virginia Journal of Law and Technology*, Fall 1997. Section IIIA.

cannot be so (in a footnote) (i)f it were, we would have expected the Supreme Court to start and end its analysis of David Paul O'Brien's burning of his draft card with an inquiry into whether he was kept warm by the ensuing flames." The court continued its discussion of the protections granted speech by stating "(t)he First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution."

The cases in question: Junger

In April of 2000 the US Court of Appeals for the Sixth Circuit heard Junger's appeal from his loss to summary judgment before the Circuit Court and found in favor of Junger. The court in (wisely) finding that source code is speech protected by the First Amendment stated:

> The Supreme Court has expressed the versatile scope of the First Amendment by labeling as "unquestionably shielded" the artwork of Jackson Pollack, the music of Arnold Shoenberg, or the Jabberwocky verse of Lewis Carroll. ... Though unquestionably expressive, these things identified by the (Supreme) Court are not traditional speech. Particularly, a musical score cannot be read by the majority of the public but can be used as a means of communication among musicians. Likewise, a computer source code, though unintelligible to many, is the preferred method of communication among computer programmers.

This language defines the issue precisely. If a computer programmer wishes to explain something to another computer programmer it is unlikely that they will do so simply in prose but will, as the court understands, include source code concerning the topic as well. Reviewing source code has been a time-honored method for passing along computer programming ideas and techniques both in and out of classrooms. In Junger's case, he sought to explain the inner workings of encryption software by posting his source code for use in a course that he was teaching.

The question is speech

It is the authors' contention that, as previously noted, the lower court in *Junger* did not understand the true nature of source code and it is this misunderstanding that resulted in source code being ruled merely functional and therefore not worthy of protection under the First Amendment. Because the court misdefined source code as merely functional they apply the O'Brien test of intermediate scrutiny and make the incorrect ruling in favor of the government. Thus having discussed the cases we revisit the core argument.

The O'Brien test of intermediate scrutiny was first established by the US Supreme Court in *United States* v. *O'Brien*, 391 US 367 (1968). The O'Brien test does not govern speech but rather actions that do not rise to the level of speech. Speech is accorded the full protection of the First Amendment but most actions are not afforded the full protection of the amendment. As the court in O'Brien stated: "we cannot accept the view that an apparently limitless variety of conduct can be labeled "speech" whenever the person engaging in the conduct intends thereby to express an idea."

The problem with applying O'Brien is that source code is not action it is speech. Source code may cause action or perhaps become action if acted upon in a compiled and called into life as a process, but this is not unlike the case with all human-readable instructions. The Sixth Circuit Court of Appeals understands this and ruled in April 2000 "(b)ecause computer code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."

As the Sixth Circuit's Court of Appeals ruling makes clear, the O'Brien test should not have been applied by the lower court in Junger but even when applying O'Brien in that case the court should have found that Junger's "actions" were protected. Mr. Justice Harlan's concurring opinion in O'Brien provides a view into what the court meant by their opinion:

> The crux of the Court's opinion is in its general statement:
>
> ... 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.
>
> I wish to make explicit my understanding that this 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. This is not such a case,

> since O'Brien manifestly could have conveyed his message in many ways other than by burning his draft card.

The above language makes it clear that O'Brien should not be used to prevent a "speaker" from reaching a significant audience with whom he could not otherwise lawfully communicate. To effectively express the ideas that make up the science of cryptography scientists must study the computer code that handles the actual encryption process and watch that code at work on computers to observe the result. While it may be argued that Junger could have published his code in the form of a book this is not so as Professor Junger's purpose in posting his code to the Internet was to show such code in action.

Given the nature of modern computing code it is quite possible to have script – a form of code – which resides on a server, viewable as text and understandable to those versed in its syntax, be interpreted "on the fly" to become working object code. This is the way that HTML, the language of the Internet, working in conjunction with a web browser works and it is how Professor Junger proposed to teach the nature of encryption software to his students. Note that Hyper Text Markup Language, and Extensible Markup Language are languages for formatting only, and it is arguable if as such they could be used to implement actions. Other codes are neither fish nor fowl, but rather interpreted codes: Jscript, Visual Basic Script. Script allows the user to edit the source code and interpret the results when viewing the code in a web browser. Script goes through the intepreter each time they are run and never compiled. Thus, given this distinction it is possible that the Court could have found that controls on encryption would be reasonable on script, if not source code. Yet, even under O'Brien the court in Junger should have found the EAR unconstitutional due to its being overbroad in its limit on speech/source. However, as the next section will show, Junger undertook to speak, to communicate, and not to act when he sought to "export" his encryption source code and thus O'Brien should not have been applied at all.

As the Sixth Circuit Court of Appeals judgment for Junger shows, the Circuit Court in Junger clearly did not understand the nature of source code. Judge James S. Gwin provides this definition of software:

> Like all software, encryption programs can take two general forms: object code and source code. Source code is a series of instructions to a computer in programming languages such as BASIC, PERL, or FORTRAN. Object code is the same set of instructions translated into binary digits (1s and 0s). *Thus, source and object code are essentially interchangeable*. While source code is not directly executable by a computer, the computer can easily convert it into executable object code with "compiler" or "interpreter" software. (Italics added)

Judge Gwin's assertion that "source and object code are essentially interchangeable" is simply wrong. His very next statement that "source code is not directly executable by a computer" exposes his error. The error in Judge Gwin's understanding of how software works is further exposed in the footnote of the previously quoted passage:

> Software in source code, a 'high level language,' is unintelligible to most, but it can be understood by computer scientists, mathematicians, programmers, and others with knowledge of the particular language in which the program is written.

Despite his disagreement with the Bernstein decision he clearly states that source code is a language that can be understood by those schooled in its intricacies.

To understand that source code is fundamentally different from object or even interpreted code one need only examine the recent Y2K crisis. Had the systems that contained the two digit date fields been open source and not proprietary compiled systems the programmers seeking to correct the field lengths would not have had to decompile and wade through billions of lines of almost indecipherable code.

Source code is critical, cross-cultural, speech as much as is mathematics. The ability to read, examine, distribute, and dispute the electronic rules are as critical today as the ability to read, examine and distribute the natural language documents that are the basis of modern industrial governance.

The cases in question: The future and federalism

While this paper is not the place to give an exhaustive account of the history and tradition of Common Law, an attempt has been made to provide a solid enough foundation upon which the reader may stand. tangent will hopefully clarify the future of the cases.

Under the common law system practiced in the United States, the principle of *stare decisis* states that once a decision (a precedent) on a certain set of facts has been made, the courts will apply that decision in cases which subsequently come before them. Thus a precedent that is binding must be followed.

A precedent is considered binding if the court that issued the ruling has the power to generate controlling decisions over the court hearing the case at hand; if it has not been overruled by a higher court or abrogated by statute; and is sufficiently analogous to the case

at hand. To determine whether the court that set the precedent is controlling in a case we must examine the relationship between each of the three layers of the Federal judicial hierarchy.

At the top of the Federal system is the US Supreme Court. The US Supreme Court is the court of ultimate decision when discussing Constitutional issues. Directly below the US Supreme Court are thirteen US Circuit Courts of Appeals, each judicially "governing" a substantial geographical area of the United States and its territories. Within each Circuit, there are United States District Courts, the federal trial courts, each state having at least one district, usually several.

The doctrine of *stare decisis* only binds courts within a single hierarchy. Each of the Federal circuits is autonomous with regard to the other circuits and therefore the decisions of the US Circuit Court of Appeals for the Ninth circuit is not precedent for the US Circuit Court of Appeals for the Sixth Circuit but is merely persuasive authority. This is why the lower court in *Junger* was able to disregard the decision in *Bernstein* and find for the Government.

Given the similarities between *Bernstein* and *Junger* it would seem to be a matter of small effort for the court in *Junger* to adopt *Bernstein*'s arguments and grant a judgment in favor of *Junger*. But, instead of following the persuasive decision in *Bernstein* the judge in *Junger* held that the *Bernstein* decision was wrongly decided and that code was not speech deserving of First Amendment protection. Because of the stark differences between the findings it is reasonable to suppose that the Supreme Court will hear the arguments.

We discuss federalism as this idea has been a guiding principle for the Supreme Court's rulings on Constitutional matters in the recent past, excluding the exceptional and unusual reasoning in *Bush* v. *Gore*. After being held secondary to Fourteenth Amendment concerns for nearly half a century the principle federalism is back in ascendance and is being applied by the Court with ever increasing frequency.

The Tenth Amendment to the US Constitution, in its entirety, provides that "the powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." This system of triple sovereignty is a fundamental and integral part of American federalism. However, the balance of power between the States Government, the Federal Government and individual autonomy is a continuos source of debate before the Supreme Court. Should the metaphor of a pendulum be used to describe this continuous debate then the ninth decade of the twentieth century was the nadir of the Tenth Amendment before the US Supreme Court. In particular in 1985, the Court in *Garcia* v. *San Antonio Municipal Transit*[22] held that States could not violate the rights guaranteed by the Federal Constitution, and negated the Tenth Amendment stating "the Constitution does not carve out express elements of state sovereignty that Congress may not employ its delegated powers to displace." The four dissenting judges characterized this opinion as reducing the Tenth Amendment to "meaningless rhetoric." Recently, however, the pendulum has reversed direction with the Court showing renewed interest in defining the limits that the Constitution places on the powers of the Federal Government.

The Supreme Court laid the groundwork for the revival of the Tenth Amendment in 1991 in *Gregory* v. *Ashcroft*[23] in which the Court emphasized that the "Constitution established a system of dual sovereignty between the States and the Federal Government." It was, however, the landmark *New York* v. *United States*[24] decision in 1992 that provided a place of pre-eminence for the Tenth Amendment. In *New York* v. *United States*[25] Court invalidated provisions of the Low-Level Radioactive Waste Policy Amendments Act of 1985 which required States to either implement federal legislative mandates or be coerced into "taking title" to the waste and subjected to liability for the waste generators' damages. The Court held that the "take title" provision was beyond the reach of Congress' enumerated powers and violated the Tenth Amendment. In its opinion, the Court articulated the following clear constitutional standard: "state governments are neither regional offices nor administrative agencies of the United States; Congress may not simply 'commandeer' the legislative processes of the States by directly compelling them to enact and enforce a federal regulatory program."

textheight 55pc The swing towards federalism continued when, three years after New York and for the first time in 60 years, the Court enforced constitutional limits on Congress' power to enact generally applicable legislation under its Article I power to regulate interstate commerce. In 1995, in *United States* v. *Lopez*[26] the Court restrained Congress from relying upon its constitutional power to regulate interstate commerce to ban the simple possession of a gun in a school zone, unless it could clearly show that such conduct involved commercial channels or interstate economic activity. In Lopez, the Court expressed concern about Congress being able to regulate all education matters, an area "where States historically

[22] *Garcia* v. *San Antonio Municipal Transit Authority*, 469 U.S. 528 (1985).

[23] *Gregory* v. *Ashcroft*, 501 U.S. 452 (1991).

[24] *New York* v. *United States*, 505 U.S. 144 (1992).

[25] *New York* v. *United States*, 505 U.S. 144 (1992).

[26] *United States* v. *Lopez*, 514 U.S. 549 (1995).

have been sovereign." The same year, in *Seminole Tribe of Florida* v. *Florida*[27] the Court completed the creation of a body of law which placed the Tenth Amendment above individual Constitutional rights by removing from individuals rights given in the Fourteenth and Eleventh Amendments. The Court limited the right of the individual to bring suit against a State in Federal court.

Other victories for federalism during the 1996–1997 term included *Vacco* v. *Quill*[28] in which the Court shifted the conflict over assisted suicide back to the States when it upheld New York (and in a related case, Washington) statutes banning physician-assisted suicide. In the first weeks of the new millennium the Supreme Court has heard one case that extends Federalism and one case that, while limiting states rights, extends the rights of the individual.

In the consolidated cases of *United States* v. *Antonio Morrison and James Crawford*,[29] the Court found the 1994 Violence Against Women Act (VAWA) to be an unconstitutional overreach of the Congress's commerce clause powers. This case is perhaps the most significant Federalism case heard in many years due to the fact that 36 states and Puerto Rico joined in a brief welcoming the VAWA as part of a joint effort between state and federal government to combat gender-motivated violence. The Court also rejected a Fourteenth Amendment argument that grants Congress the power to legislate against civil rights violations. The Court response in this case was an inverse of the Court response in the *Garcia* case, where the Fourteenth Amendment was discounted and the Tenth held to be the deciding factor. Notice that there was considerable documentation, in response to *Lopez*, that such violence had a significant effect on commerce.

In *Kimel et al.* v. *Florida Board of Regents et al.*[30] the Court held that the 1967 Age Discrimination in Employment Act (ADEA) was an unconstitutional extension of Congress' authority under section 5 of the Fourteenth Amendment. The Court held the ADEA to be unconstitutional because it abrogated the States' Eleventh Amendment immunity. This case continues the line of reasoning we first saw in *Seminole Tribe of Florida* v. *Florida*.[31] The Court further held that while Section 5 of the Fourteenth Amendment does grant Congress the authority to abrogate the States' sovereign immunity that this can only be done in the narrow confines of the remaining sections of the amendment. Since the ADEA deals with age and not one of the protected classes such as race or sex the court held that Congress acted without proper authority.

Thus the pendulum appears to be completing the arc, with the Fourteenth Amendment held as more rhetorical and the Tenth and Eleventh Amendments forming the basis for the determinations by the Justices. Given that the Fourteenth Amendment directly addresses the rights of the individual and federalism directly addresses the rights of the people's representatives at the state level the implications for the issue of encryption are particularly of interest. In this case it is the Federal Government which has limited both State and individual rights. Given that the Court has acted to protect gun ownership, strip citizens of the right to bring suit, and prevent coordinated police action to stop violence against women critics have suggested that the Court is ideological interest is in limiting the rights of the individual, not protecting the States. Advocates of federalism maintain that federalism is fundamentally on the side of individual autonomy, with state governments being closer to the people and therefore more representative of the people than the more distant federal government. In this view federalism protects the people from the excesses of a distant Federal government. Other see federalism as a movement pitting the rights of the state government against the right of the individual, and thus ensuring that for conflicts at the state level the individual has no court of last resort.

While many of the recent cases have gone against the individual bringing the case due to the underlying law or act under which the case was filed being ruled unconstitutional this may be seen either as a loss for one person or as a win for the individual autonomy as a whole. By limiting Congress the Supreme Court is can either be sending a message that the Constitution is still very much alive and that its tenets will be followed by the Court when interpreting federal legislation. Alternatively federalism can mean that the Bill of Rights does not remain in full effect, and the States have the right to undermine individuals. Federalism may mean that states rights trumps those of the individual guaranteed under the Federal law and the Constitution.

Thus, this works embodies a testable hypothesis about federalism with respect to the rights of the individual. If federalism is fundamentally about the affirmation of individual rights, then the Court will follow *Bernstein* and *Junger*. Note that this depends on accepting that source code is speech. While both the Ninth and Sixth Circuit Courts of Appeal have recognized this fact it remain arguable in theory. It will be an interesting test of a hypothesis indeed.

[27] *Seminole Tribe of Florida* v. *Florida*, 517 U.S. 44 (1996).

[28] Vacco, *Attorney General of New York, et al.* v. *Quill et al.* certiorari to the united states court of appeals for the second circuit No. 95-1858.

[29] *United States* v. *Morrison*, No. 99-5 (U.S. 05/15/2000).

[30] *Kimel* v. *Florida Board of Regents*, 120 S.Ct. 631, 145 L.Ed.2d 522 (U.S. 2000).

[31] *Seminole Tribe of Florida* v. *Florida*, 517 U.S. 44 (1996).