WRITING COMPETITION ENTRY

#6

Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web
UNM Student Writing Competition Submission
Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web

Note: A different version of this paper will be appearing in the New Mexico Law Review, Volume 33, Issue 1. The version submitted here is my own re-edit of the final version submitted to the law review prior to any law review editing. At the risk of overkill but for the sake of openness, I would like to detail the various changes in the hope that they will meet the requirements of the competition.

First, in general, this paper is my own work, not the work of the law review. There are certain changes I made to the paper on the re-edit, but except as detailed below, the changes are my own work and do not reflect input from the law review staff.

- Certain changes made to this version parallel changes I made to the law review version (such as corrections to the usage of "comprise"). This group of changes includes only those changes I made on my own, without prompting by law review staff.

- A few minor typos have been corrected (e.g., "ste" for "step"). In the law review version, these may have been corrected based on my editor spotting them. In the submitted version, they were corrected based on my either seeing them during the re-edit or catching them during an automated spell check. These instances are rare (perhaps three in the entire paper) and do not affect the substantive content of the paper.

- There were two changes to the second sentence of footnote 186 that were made in response to two words, "due process?", offered by Professor Browde after I had submitted the paper for law review edit:

  Initial version: "Current thinking seems to root privacy in equal protection, Roe, 410 U.S. at 153, though that approach suffers from the limitations that the 14th Amendment equal protection extends only to state actions..."

  Revised version: "Current thinking seems to root privacy in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, Roe, 410 U.S. at 153, though that approach suffers from the limitations that the 14th Amendment extends only to state actions..."

  Italics added to show changes. This is the only substantive change made in response to any comments received after submitting the paper for law review edit. I kept it because it makes the footnote more accurate and does not seem like a major change to the paper. If, however, the circumstances of the change would disqualify the paper for consideration, I would be glad to submit a version without that change.
- Aside from what is noted above, this paper incorporates no input from the law review. The law review files can substantiate this if there are any questions.

- There are additional changes in the law review version that, I think, improved that version. Those changes, though, were based on my editor's suggestions and are not included in this version (e.g., "comment" instead of "paper").

I hope that this version is sufficiently independent of the law review's version to permit its consideration. It is not actually the final version before law review input, but except as noted above, it is a version independent of law review input. It was prepared with the intention of staying within the guidelines for the competition, and I hope it successfully does so.

I should add that, in spite of the above, the paper definitely owes a great deal to the thoughtful, detailed, and valuable comments from Professor Baum, my faculty advisor for this paper. Regardless of this paper's eligibility for the competition, her input made a world of difference.

The truth of the above sworn to on my knowledge and by the honor code,
Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web

Thomas A. Lane

Contents

I. Introduction ............................................................................................................. 2

II. The Nature of the Web ........................................................................................ 5
    A. The Protocol Layer ......................................................................................... 6
    B. The Software Layer ...................................................................................... 12
    C. The Human Layer ......................................................................................... 16

III. The Nature of International Law ...................................................................... 19

IV. The Nature of Federalism ................................................................................. 29

V. The Nature of Non-Governmental "Law" ............................................................. 38

VI. A Case in Point: The CPPA ............................................................................. 43

VII. Preliminary Suggestions .................................................................................. 48
    A. A Role for International Law ......................................................................... 48
    B. A Role for Federal Law .................................................................................. 51
    C. A Role for State Law ..................................................................................... 61
    D. A Role for Non-Governmental Law ............................................................... 65
    E. A Role for Hybrids ....................................................................................... 68

VIII. Summary .......................................................................................................... 69
I. Introduction

Federalism is a fact of U.S. law. It might be viewed as a "sacred cow," or more generously as "a value that deserves independent consideration," or more simply as a "first principle." But it is a fact, and it is within the framework of federalism that U.S. law will be developed and applied to the Internet and World Wide Web.

This paper argues that federalism is in fact particularly well suited to the development of law for the Web. It may be "one world, one Web," in the sense that the

---


4 For this paper, "Web" will be used in a generic sense to refer to the World Wide Web itself, the underlying Internet, and the related functions such as electronic mail and newsgroups. Where distinctions among the types of functions are needed, the paper will use more precise terminology. In general, though, the Web is the interface through which most users access and experience the various aspects of the Internet.

5 For this paper, "law" is viewed in a broad sense. It includes governmental law, such as statutory and common law, as well as non-governmental sources of regulation, control, or influence, such as the voluntary technical standards developed by the World Wide Web Consortium (W3C).
Web is a globally shared resource. Such a perspective suggests that it would be beneficial to have areas of law that are consistent internationally. But it is also "a world of Webs," with multiple interconnecting but distinct networks, multiple interacting groups of users, and multiple and diverse potential legal issues. This approach suggests that a diversity of local law would be beneficial in certain areas as well.⁶

The conflict between, on the one hand, a pressure for consistency in Web law and, on the other, a role for diversity creates the first underlying theme of this paper. There is no single answer for how to best apply law to the Web. The legal tool best suited for deterring child pornography differs from the legal tool best suited for establishing a standard of care for tort negligence on the part of Web site operators.

The second underlying theme is that the Web, though a fundamentally new way of communicating among people, is nevertheless a human creation. Its newness suggests that new law will, at times, be appropriate. Its human roots, in turn, suggest that much existing law can be applied to the Web, with varying degrees of modification. Some new legal tools may need to be created, but many old tools remain viable.⁷

---

⁶ Obviously, "local" in a Web sense is not the same as "local" in a geographic sense. State boundaries are not always the best way to segregate issues related to the Web. In some instances, though, state boundaries remain meaningful. For example, nothing about the nature of the Web suggests that a business license for an Internet Service Provider (ISP) should be any different from licenses for more traditional neighboring businesses.

U.S. federalism is flexible enough to accommodate law from many sources: international, federal, local, and non-governmental. Federalism can adapt existing law to new situations while concurrently providing avenues for the creation of new law. The Web creates a diversity of legal needs; federalism offers a diversity of legal tools.

This paper offers a general exploration of the federalist legal toolbox, as currently and potentially applicable to the Web. The paper begins with overviews of the nature of the Web, international law, the federalist system, and non-governmental sources of regulation. Against this backdrop, the paper examines the recent U.S. Supreme Court ruling on the constitutionality of the Child Pornography Prevention Act (CPPA), an act that demonstrates both successes and failures in applying federal law to the Web. Finally, the paper offers suggestions regarding which source of law—international, "cyberspace" has value as a distinct discipline, or whether it might be better left to the existing tools of law).

8 In the U.S. federalist scheme, international law is applied within the country through internal U.S. mechanisms such as treaty ratifications. See infra text accompanying notes 64 & 65.


10 In criminalizing the distribution of actual child pornography via the Web. See infra text accompanying note 155.

11 In attempting to criminalize the distribution of virtual child pornography via the Web. See infra text accompanying notes 151 & 152.
federal, state, or non-governmental—is best suited to addressing particular legal issues regarding the Web.

II. The Nature of the Web

By now, certain observations about the Web are very nearly truisms. The Web is global in scope, extending to all seven continents. A population of users is quick to proclaim the independence and ungovernability of the Web. Some users take advantage of the perceived anonymity of the Web to escape behavioral constraints of the "real world." Combined, these factors can lead to an impression of a "Wild Wild Web," an electronic version of lawless Old Tombstone in the days of the O.K. Corral.

Such an impression is, however, flawed. As Lawrence Lessig has pointed out, there are multiple mechanisms for applying law to the Web. Once identified, individual

12 See, e.g., Yahoo! listing of Web sites by region, at http://dir.yahoo.com/Regional/Regions/ (leading to links such as live Webcasts from Antarctica).

13 See, e.g., Lawrence Lessig, Code and Other Laws of Cyberspace 4-5 (Basic Books 1999) [hereinafter Lessig II] (describing the perception that the Web "could only be free").

14 See, e.g., id. at 14-17 (discussing "Jake" who posted "graphic and repulsive" stories to the alt.sex.stories newsgroup).

15 Id. at 30-42 (discussing "architectures of control").
users can be brought before court. The software can utilize authentication and authorization to identify users and control access to content and permissible activities. The underlying protocols themselves can be altered to control activity.

A. The Protocol Layer

At its core, the Web is not beyond regulation; at its core, it is simply a collection of protocols. The basic Internet protocols are processing and formatting rules that

---


Authentication and authorization are related, but distinct, actions. Authentication establishes the identity of a user; authorization controls what that user, once identified, is permitted to do. Authentication is the key to a doorlock; authorization, the size of the room behind the door. See, e.g., Cisco Systems, "authentication" and "authorization," in Internetworking Terms and Acronyms, available at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/a12.htm.

See Lessig II, supra note 13, at 51-53 (describing the effects of regulating code, including the limitations of the likely resistance).

Beneath the protocols, there are two additional layers. The first is the hardware, the machinery and wiring of the various computers and connections that constitute the physical foundation for the Web. The second layer is composed of the operating systems, such as Windows or Unix, that enable the hardware to understand and process the
enable computers to communicate with each other across a series of interconnected but independently operated computer networks. The Web, in turn, is an overlay of protocols that make it simple for users to navigate and use the underlying Internet. Added to the mix are a variety of file format protocols that enable a receiving computer to communicate to its user what the sending computer has sent, including text, images,

Internet protocols. Neither of these layers is unique to the Web, and the legal issues regarding both are beyond the scope of this paper.


and movies. A separate group of protocols addresses security-related concerns such as encryption and authentication.

These protocols can be separated into global protocols, public protocols, and private protocols, each of which warrants separate legal consideration. Global protocols are those which every user's machine must support if that user is to utilize the Web at all. The most obvious example is the Internet Protocol (IP); if a user's machine does not support this basic protocol, then no communication across the Internet is possible.

A global protocol demands global definition, but it conversely invites little legal intrusion. Because the protocol must be followed in order to use the network, there is little that the law can add in terms of coercion or deterrence. Furthermore, in order to be

24 See, e.g., MPEG-2 FAQ § 1 What is MPEG? (Berkeley Multimedia Research Center), at http://bmrc.berkeley.edu/frame/research/mpeg/mpeg2faq.html.


28 This is a bit of an overstatement. Protocols other than IP can be used to communicate over limited portions of the infrastructure underlying the Web, if that infrastructure is specially configured. Standard IP is needed, however, to communicate across the overall global resource that is the Web.
global, these protocols must be made public, thereby ensuring independent review of their effectiveness and trustworthiness.\(^{29}\) International technical organizations already exist for the development and publication of global protocols.\(^{30}\) There is little that government could add to what these groups are already doing, and the direct specification of global protocols stands as a clear example of an area where government should not interfere.

Public protocols are those which are openly published and which a user needs to adopt in order to perform a particular action, but which the user need not adopt unless he/she chooses to perform that action. For example, the Internet Relay Chat Protocol (IRC)\(^ {31}\) is openly published and supported by a number of different products.\(^ {32}\) A user who chooses to participate in an IRC chat room must have IRC-supporting software installed, but a user has no need for such software if he/she chooses not to participate in a

---

\(^{29}\) An ongoing theme in this paper is that protocols and software that are exposed to public review are less likely to contain hidden viruses, bugs, or vulnerabilities, because a large number of independent readers will have had the opportunity to review them for just such flaws.

\(^{30}\) E.g., IETF, homepage at http://www.ietf.org; W3C, homepage at http://www.w3c.org.


chat room or if he/she prefers a chat room based on a different protocol (such as AOL Instant Messenger).

In general, a public protocol seems to invite almost no legal control. It is openly published, so any hidden viruses should be easily exposed. It does not require global conformity, since it is only used by a sub-group of users. It is not subject to monopolization, since anyone who chooses to write a program to support it can do so. Absent some sort of complicating issue, there seems little reason to interfere.33

A private protocol is a privately owned, unpublished protocol. In general, a user who wishes to use the protocol must obtain software from the owner of the protocol. An obvious example is the file format used for Microsoft Word; a user who wishes to create,  

33 One such complicating issue has involved the national security concerns associated with encryption software based on public protocols such as Secure Socket Layers (SSL). See, e.g., Computer Science and Telecommunications Board, National Research Council, Cryptography's Role in Securing the Information Society ch. 4 Export Controls (National Academy Press 1996), available at http://www.nap.edu/readingroom/books/crisis/chapter4.txt (discussing the use of export controls for encryption software under the Arms Export Control Act (AECA) of 1949 and the Export Administration Act (EAA)). The complete text of the report is available at http://www.nap.edu/readingroom/books/crisis/.
view, or edit a document in this format must generally obtain software from Microsoft itself.34

From the outset, a private protocol becomes a subject of law. The creation and fixation of the protocol invokes copyright;35 any misappropriation of the private protocol would be subject to copyright remedies.36 Furthermore, because the private protocols are secret, there is no opportunity for independent readers to verify whether there might be hidden vulnerabilities or other flaws embedded within the protocol itself. The possibility

34 The alternatives are to obtain software from a manufacturer licensed by the protocol owner, to obtain pirated copies of the software, or to obtain a legally "reverse engineered" compatible product. For a discussion of software piracy, see Eric H. Holder, Jr., Remarks at a Press Conference Announcing the Intellectual Property Rights Initiative (July 23, 1999), available at http://www.cybercrime.gov/dagipini.htm; for a discussion of reverse engineering and its legal protections under the "fair use" doctrine of U.S. copyright law, see Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (1993).

35 Copyright law also protects global and public protocols, but because they have been made freely available, there is no cause of action if they are in fact used. There may, however, be a cause of action if a global or public protocol is modified into a private protocol and then used for profit.

36 Subject to the "fair use" exception for reverse engineering. Supra note 34.
of such vulnerabilities or flaws, in turn, creates the potential for actions under both contract and tort.\textsuperscript{37}

B. The Software Layer

On top of the protocols themselves, there are the various software programs used to implement the protocols. One major division among software programs is between open-source software, whose underlying human-readable source code is made readily available to the public,\textsuperscript{39} and private, proprietary software, whose source code is guarded as a trade secret. There is a further distinction among the proprietary software between "shareware," which is freely distributed but which users are expected to voluntarily pay

\textsuperscript{37} The product did not perform as advertised. See \textit{U.C.C.} § 2-314 (1989) (defining an implied warranty of merchantability).

\textsuperscript{38} The product caused harm. See \textit{Restatement (Second) of Torts} § 6 cmt. a (1965) (a general explanation of types of tortious conduct).

\textsuperscript{39} See, \textit{e.g.}, Free Software Foundation, at \url{http://www.gnu.org/ fsf/fsf.html}. 
for, and what is sometimes called "shrinkware,"\textsuperscript{40} which frequently comes in shrink-wrapped packages and which users must pay for before the software can be installed.\textsuperscript{41}

As with the underlying protocols, the software that is the most open and public invites the least legal intrusion. The more accessible the source code, the better the opportunity for independent readers to ensure that it lacks hidden viruses and will in fact

\textsuperscript{40} "Shrinkware" is a descriptive term used by the software development community. It was used, for example, by Stuart Anderson in response to the first question from the audience at a meeting of the Florida Linux User Xchange. At http://www.flux.org/linux/lsb.html. It is also used by Lou Grinzo in the final paragraph of "Lowering the Net for Open Source." Dr. Dobb's Journal, September 20, 1999, available at http://www.ddj.com/documents/s=891/ddj9975o/9975o.htm.

\textsuperscript{41} Some software is a hybrid. The Linux operating system, for example, is open-source software, but companies such as Red Hat offer shrinkware versions of Linux. Red Hat takes the open-source Linux, certifies it, compiles it into machine-readable form, puts it onto convenient CDs, shrinkwraps the package, and provides customers with technical support. Users who purchase shrinkware Red Hat Linux are paying for the convenience that results from Red Hat's services, not the Linux itself. Linux remains open source, while Red Hat Linux remains shrinkware. See Red Hat Linux Operating System, at http://www.redhat.com/software/linux/.
perform as advertised.\textsuperscript{42} The better the opportunities for correcting potential problems before they become problems, the lower the need for legal interference.

Conversely, the software that is least open to public review--private software, whether shareware or shrinkware--has a high potential need for legal control. When the source code of software is not open to independent review, the users lose their independent source of protection against hidden viruses, bugs, or other "undocumented features."\textsuperscript{43} This loss of before-the-fact informal protection increases the potential need

\textsuperscript{42} In theory, the openness of source code also makes it easier for malicious hackers to discover security holes within the software. In practice, however, if malicious hackers can find the security holes, so can benevolent security professionals who are quick to communicate the flaw to others so that it can be corrected before it is exploited. For example, as Linux gained popularity, a series of security holes were rapidly exposed and communicated, along with fixes as they became available. See, e.g., the following advisories dealing with Linux from the Computer Emergency Response Team (CERT) at Carnegie Mellon University: CA-1999-03 FTP Buffer Overflows, at http://www.cert.org/advisories/CA-1999-03.html; CA-1998-12 Remotely Exploitable Buffer Overflow Vulnerability in mountd, at http://www.cert.org/advisories/CA-1998-12.html; CA-1998-05 Multiple Vulnerabilities in BIND, at http://www.cert.org/advisories/CA-1998-05.html.

\textsuperscript{43} "Undocumented feature" is an informal euphemism for software performing in unexpected ways, regardless of the degree of inconvenience and/or damage the unexpected behavior causes.
for after-the-fact legal protection, which in turn invites the potential application of contract law,\textsuperscript{44} tort law,\textsuperscript{45} and perhaps personal property law.\textsuperscript{46}

Furthermore, a tort negligence action against a provider of private software might be appropriate if software is sold that lacks adequate security. The first step here would be a fact pattern where a hacker exploited a security flaw in the software to gain access and cause damage to a user's computer. The next step would be to establish that the user had a reasonable expectation that such harm would not occur. The third step would be to establish that the software provider had a duty to provide reasonably secure software, that the provider failed to meet its reasonable standard of care in incorporating security into the software, and that the lack of reasonable care was a proximate cause of the damage to the user's computer. From this pattern might flow a tort negligence action, which in turn might encourage providers of private software to improve their attention to security.\textsuperscript{47}

\textsuperscript{44} \textit{Cf.} supra note 37 (contract for private protocols).

\textsuperscript{45} \textit{Cf.} supra note 38 (tort for private protocols).

\textsuperscript{46} Perhaps through conversion, for example, if a hidden virus has caused the user's machine to be used in ways that the user did not want. \textit{See infra} note 206.

\textsuperscript{47} Consider the following scenario: A major software provider offers an upgrade to a popular email program. Users adopt the upgrade. A student in Southeast Asia sends out an email message containing an attachment that exploits a vulnerability in the email
C. The Human Layer

On top of the layers of protocols and software, there are the people who use the Web. Such people may be individuals or members of groups or employees of corporations which have a distinct legal "personhood." They may be users who seek the content and services available on the Web, providers of such content and services, operators who run the sites that the Web comprises, or any combination of the above.


The student who wrote the "I Love You" virus was prosecuted in the Philippines, but a question that was not addressed was whether the manufacturer of the software, Microsoft in this case, might be held liable under tort negligence for offering an email product which permitted such widespread harm to be done. The manufacturer would likely put forward a defense based on warranty limitations, but that defense can fail if the limitations are found to be unconscionable. Restatement (2d) Contracts § 208; Uniform Commercial Code § 2-302.

48 See, e.g., Louisville, C. & C. R. Co. v. Letson, 43 U.S. (2 How.) 497 (1844); Marshall v. Baltimore & O. R. Co., 57 U.S. (16 How.) 314 (1853). Under these cases, a corporation is a "person" in a Constitutional sense even though it is not a "citizen"; the corporation can sue and be sued, but it cannot vote.
They may access the Web through a typical browser, or they may employ software such as "spiders" to automatically search the Web and gather content on their behalf.

Whatever the case, the common denominator is that these are people, humans, with all the associated behaviors.

Such behaviors range from the perfectly legal and arguably praiseworthy to the criminal. In the middle ground, Web users seem to display all of the characteristics of human behavior, subject on the one hand to the physical constraints of Web technology, but on the other hand sometimes emboldened by the Web's shortage of behavioral

49 Software that automatically searches across Web sites.

50 Such as the Wildlife Conservation Society's efforts to promote conservation through its Web site, at http://www.wcs.org/, or the United Nations' and U.S. Congress' efforts to promote the accessibility of law, at http://www.un.org/ and http://thomas.loc.gov, respectively.

Law, in its various manifestations, only exists in response to human behavior. Because human behavior is exhibited on the Web, law for the Web, whether new or adapted, becomes necessary. Legal actions so far have included the tort of defamation, copyright infringement, and crimes such as unauthorized access and harm to computer systems. There is no reason to expect that actions will stop there; rather, there is ample reason to believe that torts for the Web will eventually expand to test such areas as negligence, negligent infliction of emotional distress, and loss of consortium. There are likely to be actions testing new areas of contract and property.

52 See supra note 14.


56 E.g., United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

57 For example, if an ISP fails to adequately protect a user's personal private information from outside hackers, there may be a malpractice-type action. See infra note 124.

58 For the purposes of the bystander rule, it is unclear who is a "bystander" in the context of the Web or what the Web equivalent of "contact" is.
The diversity of the Web itself, and the diversity of its users' behaviors, suggests that a diversity of law is needed to address the issues that arise. A diversity of law, in turn, suggests a diversity of legal mechanisms. This need for diversity supports the proposition that the U.S. system of federalism is particularly well suited to the development of law for the Web.

III. The Nature of International Law

In the modern world, international law provides the broad framework within which national law operates. The U.S. may be the world's lone remaining superpower, and it may be slower than other countries in adopting specific international agreements such as the Kyoto Protocol\(^{62}\) or the Rome Statute of the International Criminal Court.\(^{63}\)

---

\(^{59}\) It is unclear what "consortium" might be within the Web and whether its loss can be considered a legal harm.

\(^{60}\) It is unclear how to apply the Hadley v. Baxendale rule of foreseeability/implied consent to transactions conducted on the Web.

\(^{61}\) There may be a conversion aspect to a hacker wrongfully using another user's account. See infra note 206. Also, it is unclear whether a "cyber-squatter" can use a trademarked Web address for long enough and actively enough to establish adverse possession.


Still, the U.S. is a member of the international community, and international law provides the framework for U.S. law.

International law is incorporated into U.S. federalism through various mechanisms, primarily operating at the federal level. For example, both treaties\(^{64}\) and implementing legislation can be used to incorporate international agreements into federal law,\(^{65}\) thereby bringing such agreements within the scope of the supremacy clause.\(^{66}\) Furthermore, both state and federal courts can hear cases based on international law.\(^{67}\) International law therefore plays a role in the U.S. federalist scheme.

---

\(^{64}\) E.g., U.N. Charter, 59 Stat. 1031 (1945) (treaty ratified by Senate).


\(^{66}\) U.S. Const. art. VI.

\(^{67}\) E.g., 28 U.S.C. § 1605 (2002) (which codifies a U.S principle that even foreign countries can be subject to federal or state courts in certain circumstances); Christopher v. Harbury, 122 S. Ct. 2179, 2185-2190 (2002) (where federal court considered international law in tort action against CIA); Price v. Socialist People's Libyan Arab Jamahiriya, 294 F.3d 82, 98-99 (D.C. Cir. 2002) (federal court stating, "We would break with the norms of international law and the structure of domestic law were we to extend a constitutional rule meant to protect individual liberty so as to frustrate the United States government's clear statutory command that Libya be subject to the jurisdiction of the federal courts in the circumstances of this case"); Register of Wills v. Arrowsmith, 778 A.2d 364, 378-381 (Ct. App. 2001) (where state court considered international law
Because the Web is an international resource, there is an immediate appeal to the idea of using international law to govern it. In theory, this would provide for global consistency, enabling, for example, a Calcutta businessman to perform transactions across the Web with a consistent set of expectations regarding the validity and enforceability of the contracts behind such transactions. Such an ideal would conceivably carry many benefits.

In fact, however, international law has limitations. It is primarily a law among nations, not a law among individuals. It is rooted in the Treaty of Westphalia,\(^68\) which in turn is based on concepts of national sovereignty. Each country becomes a legal entity under international law, akin to the way that corporations became legal "persons" under U.S. law during the nineteenth century.\(^69\)

\(^{68}\) Peace Treaty Between the Holy Roman Emperor and the King of France and their Respective Allies, October 24, 1648, available at http://www.yale.edu/lawweb/avalon/westphal.htm.

\(^{69}\) E.g., Louisville, C. & C. R. Co. v. Letson, 43 U.S. (2 How.) 497 (1844); Marshall v. Baltimore & O.R. Co., 57 U.S. (16 How.) 314 (1853). These decisions were rooted in the fact that a corporation needed to be a "person" in a constitutional sense in order to sue, be sued, or, as a consequence, obtain constitutional protections. Similarly, a nation must be a
International law has been extended to the activities of individuals, but only in certain cases. If an individual’s actions can be attributed to a state, then that state can be held liable for those actions.\textsuperscript{70} If an individual has violated \textit{jus cogens}\textsuperscript{71} norms of international law, then that individual can be held accountable under international law, but such \textit{jus cogens} norms have, so far, extended only to widely recognized as wrongful acts such as piracy,\textsuperscript{72} genocide,\textsuperscript{73} war crimes such as torture or taking of hostages,\textsuperscript{74} and crimes against humanity such as murder or enslavement.\textsuperscript{75} Nothing on the Web has legal entity in order for it to enter into treaties or otherwise operate within the framework of international law.


\textsuperscript{71} "A mandatory norm of general international law from which no two or more nations may exempt themselves or release one another." \textit{Black's Law Dictionary} 864 (7th ed. 1999).


\textsuperscript{73} Rome Statute of the International Criminal Court, \textit{supra} note 63, Part 2, art. 6.

\textsuperscript{74} \textit{Id.}, art. 8.

\textsuperscript{75} \textit{Id.}, art. 7.
approached such levels of harm, though it seems plausible that some actions eventually might.\textsuperscript{76}

The agencies of international law have a similar bias in favor of state actions and against individual actions. The founding statute of the International Court of Justice (ICJ) requires that nations be parties to actions brought before it.\textsuperscript{77} An individual who seeks to bring an action in this framework must first convince his/her government to bring an action on his/her behalf. Government intervention on behalf of individual citizens is far from automatic.\textsuperscript{78} Other international courts, such as the International Criminal Tribunal for example, included a hypothetical where a hacker from one country used the Internet to hack into and disable another country's rail scheduling system, leading to the collision of two trains and the deaths of hundreds of crew and passengers. \textit{Available at} http://www.ilsa.org/jessup/jessup02/problem.html. As reliance on the Web continues to grow, so does the possibility that a Web-based attack can lead to significant physical harm, thereby moving closer to the realm of crimes against humanity.

\textsuperscript{76} The problem for the 2002 Philip C. Jessup International Law Moot Court Competition, for example, included a hypothetical where a hacker from one country used the Internet to hack into and disable another country's rail scheduling system, leading to the collision of two trains and the deaths of hundreds of crew and passengers. \textit{Available at} http://www.ilsa.org/jessup/jessup02/problem.html. As reliance on the Web continues to grow, so does the possibility that a Web-based attack can lead to significant physical harm, thereby moving closer to the realm of crimes against humanity.

\textsuperscript{77} Statute of the International Court of Justice (I.C.J.), art. 34, para. 1, June 26, 1945, 3 Bevans 1153, 59 Stat. 1055, 1059.

\textsuperscript{78} Note the difficulties that the Berenson family has had in seeking U.S. government assistance in the case of Lori Berenson, held in Peru. \textit{See}, \textit{e.g.}, CNN, \textit{Court in Peru Upholds Berenson Sentence}, Feb. 18, 2002, \textit{at} http://www.cnn.com/2002/WORLD/americas/02/18/berenson.peru/index.html.
for the Former Yugoslavia, do bring actions against individuals, but their creation requires action by the United Nations, which in turn requires agreement among multiple countries. Such mechanisms seem designed to deal with specialized, relatively short-term problems, and they do not seem likely to offer an individual plaintiff anything resembling "speedy relief."


81 During the writing of this paper, the founding statute for the International Criminal Court (I.C.C.) went into effect. Supra note 63. It seems yet too early to offer a balanced assessment of the I.C.C. The goals are laudable and there is reason to hope that the court can succeed at offering a permanent neutral forum for crimes such as war crimes. There are, however, two significant limitations. First, the court's jurisdiction is limited to major crimes, which would exclude civil actions and all but the most egregious Web crimes. And second, the U.S. is not a signatory to the I.C.C. treaty. Absent U.S. cooperation, any sort of tribunal will face serious difficulties in applying any sort of law to the Web. See U.N., Rome Statute of the International Criminal Court: Overview, at http://www.un.org/law/icc/general/overview.htm; Communication from U.S. Government to U.N. Secretary General, May 6, 2002 ("This is to inform you, in connection with the Rome Statute of the International Criminal Court adopted on July 17, 1998, that the United States does not intend to become a party to the treaty"), available at
Individual actions under international law can, however, be brought in municipal courts. Historically, municipal courts have been prominently used to prosecute piracy, which has long been recognized as an international crime and which has a long tradition of being prosecuted in whatever municipal court happens to establish personal jurisdiction over the defendants. The difficulties in municipal courts are threefold: first, the international law must be established; second, the court must establish personal jurisdiction over the defendant; and third, the court must be able to enforce meaningful relief for the plaintiff, should judgment be found in plaintiff’s favor.

The first of these prongs, defining the law, might on its face seem the easiest to establish, but even it invites problems. International law is not like the common law, in that international law relies on the behavior of and agreements among nations rather than prior judges’ interpretations of specific situations. There is not stare decisis as the


82 In international law, “municipal courts” include all courts within a country, including, within the U.S. system, city, county, state, and federal courts.

83 See, e.g., Restatement (3d) of the Foreign Relations Law of the U.S. § 522 cmt. c (“Any state may seize a ship or aircraft on the high seas on reasonable suspicion of piracy, arrest the suspected pirates, seize the property on board, try the suspected pirates, and impose penalties on them if convicted.”).

84 See, e.g., Statute of the I.C.J., supra note 77, art. 38 (which excludes previous decisions of the I.C.J. from the available sources of law).
common law knows it. This leads to an unwieldiness and lethargy in developing new law. For example, the International Law Commission (ILC) has been working on the Responsibility of States for Internationally Wrongful Actions\textsuperscript{85} for more than 50 years. Although the current draft is a praiseworthy expression of what international law on the subject should be, it remains a draft, not yet adopted by the General Assembly, and not yet carrying anything more than persuasive force under international law.\textsuperscript{86} The Web will not wait 50 years for its law to be developed.\textsuperscript{87}

Of the three prongs, if defining the law is in fact difficult, the next two, establishing personal jurisdiction and enforcing a judgment, can approach impossibility. Personal jurisdiction would depend upon the cooperation of the defendant or his/her home country,\textsuperscript{88} and enforceability would depend on a variety of factors. Enforcement of

\textsuperscript{85} RSTWA, supra note 70.

\textsuperscript{86} Statute of the I.C.J., supra note 77, art 38.

\textsuperscript{87} In exceptional circumstances, the United Nations can at times develop general principles of international law quite rapidly, as evidenced by its various resolutions against terrorism. E.g., Human Rights and Terrorism, G.A. Res. 160, U.N. GAOR, 56th Sess., U.N. Doc. A/RES/56/160 (2002). Such rapid-fire resolutions suffer, however, from generality, vagueness, and, in the case of terrorism, a certain circularity of definitions, which would make it difficult to enforce the resolutions in any but the most blatant circumstances.

\textsuperscript{88} "Home country" is a simplification. Depending on circumstances, it might mean the country where the defendant is domiciled, resident, or physically present. The basic idea
criminal incarceration would require either physical custody over the defendant or the cooperation of the defendant's home country; enforcement of monetary criminal penalties or civil damages awards would require the cooperation of either the defendant or the country where his/her money or property is located; and enforcement of equitable remedies would require the cooperation of the defendant's home country.

For example, in a U.S. municipal court, personal jurisdiction over an alien defendant would depend on whether the defendant had "substantial contacts" with the forum court's state. If an Arizona customer purchases a defective product from a French firm's Web site, and if the customer then brings action in an Arizona court, the issue of personal jurisdiction would turn upon whether the French firm's volume of business with Arizona was substantial enough to establish personal jurisdiction. Enforcement by a municipal court would depend upon some combination of personal custody of the

is that the "home country" is the country which can, at a particular time, establish physical jurisdiction over the defendant.

89 "Alien" in the U.S. system meaning a citizen of either another state or another nation.

90 "Substantial contacts" is, of course, a shorthand way of expressing the far more complex series of tests that have evolved from International Shoe Co. v. Washington, 326 U.S. 310 (1945), and its progeny.
defendant, cooperation of the defendant, or cooperation of the defendant's home country or the country where the defendant's money or property is located.

The difficulties do not, however, mean that international law cannot be useful for the Web. Certain areas of law for the Web can be based on already established international law. One clear example here is copyright law, where the Berne Convention has already provided a multinational framework for interpretation of copyright issues. Cases involving parties from different countries have already established that copyright can be extended to the Web. Such cases have already proven that international law has a role in the application of law to the Web.

---

91 Such cooperation on the part of the defendant might be motivated, for example, by a defendant's desire to continue doing business within the U.S.

92 Such cooperation among countries is not automatic. See, e.g., Yahoo!, Inc., v. La Ligue Contre le Racisme at L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (where a U.S. federal court refused to enforce an order from a French court).


The initial foothold in areas such as copyright might be extended into other areas, such as areas of contract. Such law might be developed through bilateral agreements, multilateral agreements, or U.N. resolutions. In spite of the difficulties inherent in developing and applying international law, there can be areas where international law is a useful tool for addressing legal issues regarding the Web.

IV. The Nature of Federalism

As a starting point, U.S. federalism is a fluid, dynamic, and somewhat ambiguous concept. A "federal" system is a system that gives power to the various states, while a "federal" statute takes power away from the states and exercises power by the central government. To avoid such ambiguities within this paper, the words "federalist" or "federalism" will refer to the system and theory of federalism, while the word "federal" will refer to the central government.

Justice Brandeis famously suggested that sometimes the fact of the law is more important than the correctness of the law, especially when various parties have come to a U.S. company for, among other things, electronically transmitting to Japan translations of protected works).

This paper later suggests that it might be useful to develop a general U.N. resolution for a "bill of rights" for Internet consumers. Infra Part VII.A.


This approach leads to some awkwardness. "Federalist system" sounds less graceful than "federal system." Hopefully, clarity can overcome the awkwardness.
rely on a particular interpretation. During the same term of the Court, the same Justice also famously suggested that a strength of federalism is that it creates room for experimentation among the states. The second principle's room for experimentation creates instability and unpredictability, directly counter to the first principle's emphasis on stability and predictability. Although contradictory, both principles hold value for the Web.

On the one hand, a business that is considering whether to open a Web site and, if so, how its site will operate would benefit from having hard, established law to factor into its consideration. An individual who likes to "experiment" on the Web would benefit by knowing in advance which "experiments" are legally acceptable and which are not. Potential victims of abuse might be better protected by stable law. All of the above argue in favor of hard, established law.

On the other hand, many aspects of the Web do not yet seem ready for hard law. Although the dissemination of child pornography across the Web is widely

98 Burnet v. Coronado Oil & Gas Co., 285 U.S. 393, 406 (1932) (Brandeis, dissenting) ("[I]n most matters it is more important that the applicable rule of law be settled than that it be settled right.").

99 New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").
condemned,\textsuperscript{100} attempts to control access to pornography by minors on the Web have run afoot of fundamental First Amendment protections.\textsuperscript{101} Similarly, within the environment of an online chat room, it may not be simple to determine when "flaming"\textsuperscript{102} is parody, defamation, or a harmless venting of emotion.\textsuperscript{103} These examples suggest that there are

\begin{footnote}{\textsuperscript{100} See supra note 51, and infra Part VI.}
\textsuperscript{101} See infra Part VI. From one perspective, this example might be viewed as a conflict between two sources of hard law, federal legislation and the federal Constitution. For the purposes of this paper, though, the example is better viewed as an illustration of a need for experimentation to determine which sort of hard legislative law, when applied to the Web, will align with the fundamental U.S. values expressed in the Constitution.
\textsuperscript{102} Messages that abuse another user.
\textsuperscript{103} Hustler said Jerry Falwell had sex with his mother in an outhouse. Falwell objected, but because the statement was found to be parody, Hustler's right to say it was protected. Hustler Magazine v. Falwell, 485 U.S. 46 (1988). Matt Drudge said Sidney Blumenthal beat his wife, but because the statement was not parody, Drudge was not protected. Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998). On a continuum between parody and assertions of fact, it is not clear where a flame in a chat room would fall. Most likely, the flame would not pretend to be thoroughly researched or authoritative, which would push it toward the protections of parody. But it would probably present itself as if it were an assertion of fact, which would push it away from those protections. Because the issue is unclear, multiple attempts at resolving it on a fact-specific basis might uncover general principles which could then be applied to later cases.}
areas where it may be beneficial to avoid hard law and take advantage of the flexibility of experimentation.

U.S. federalism is rooted in the fact that, after the Declaration of Independence but before the U.S. Constitution, each of the states considered itself a sovereign nation.104

104 Articles of Confederation, March 1, 1781. Note the distinction between confederation and federation.

There is the view that the U.S. version of sovereignty was intended to turn the English concept of sovereignty on its head. Rather than the English model, where sovereignty was historically rooted in the divine infallibility of the monarch, the U.S. model in this view is rooted on the sovereign power of the people, portions of which the people choose to assign to the state or federal governments. See, e.g., Seminole Tribe of Florida v. Florida, 517 U.S. 44, 150-155 (1996) (Souter, dissenting); U.S. Term Limits, Inc., v. Thornton, 514 U.S. 779, 838-839 (1995) (Kennedy, concurring).

The distinction between this "sovereignty in the people" approach and the more traditional "sovereignty in the states" approach has led to vigorous discussions regarding the 11th Amendment limits of federal jurisdiction. See, e.g., Seminole Tribe. The distinction also holds the possibility of interesting discussions about how the Constitution, in more general terms, should be applied to the Web. If sovereignty is rooted in the people, then the Constitution becomes an instrument whose primary purpose is to protect the interests of the people, which in turn suggests an expansive view of Constitutional protections offered to Web users. If, however, sovereignty is rooted in the states, then the Constitution becomes an instrument whose primary purpose is to protect
Each state had plenary power, which it could divide and assign as it chose. The original states agreed to assign certain limited powers to the central government, while retaining other powers to themselves. Of the retained powers, some, in turn, were assigned to the counties and municipalities within each state.105

Early attempts at expanding the power of the central government were mixed in their results.106 The Civil War amendments107 brought a fundamental shift toward federal state interests from intrusions by the federal government, which in turn suggests a more restricted view of Constitutional protections for Web users.

How this distinction might affect the development of Constitutional law for the Web has the potential of being significant, but it is beyond the scope of this paper. For the purposes of this paper, it is sufficient that traditional U.S. jurisprudence is based on the "sovereignty in the states" approach, that states held plenary power prior to the Constitution and assigned a portion of that power to the central U.S. government.

105 Examples are the power for counties to establish sheriff's departments and the power for municipalities to establish real estate zoning regulations.

106 Chisholm v. Georgia, 2 U.S. (2 Dall.) 419 (1793), asserted federal court jurisdiction over the individual states, which quickly led to the Eleventh Amendment, denying that power. McCullough v. Maryland, 17 U.S. (4 Wheat.) 316 (1819), in turn, asserted a federal authority over central banks, free of state taxation, an authority that survived. See Osborn v. Bank of the United States, 22 U.S. (9 Wheat.) 738 (1824). Worcester v. Georgia, 31 U.S. (6 Pet.) 515 (1832), asserted that only the federal government held authority over Indian tribes, which led to President Jackson's apocryphal statement along
power, at the cost of state power. After initial Supreme Court rulings that seemed to limit
the scope of the Civil War amendments, the series of rulings, combined with
Congressional activity, expanded the power of the federal government during the New
Deal, World War II, and the Civil Rights period. The Court has since appeared to be
limiting central authority in some areas, while expanding it in others.

the lines of "John Marshall has made his decision; now let him enforce it" (reported with
variations in various sources). See, e.g., Felix S. Cohen, Handbook of Federal Indian
Law 83 (1982); Grace Steele Woodward, The Cherokees 171 (Univ. of Okla. Press
1963); Horace Greeley, American Conflict 106 (1864).

Especially the Fourteenth Amendment with its explicit grant of power to Congress
over the states in Section 5.

E.g., Civil Rights Cases, 109 U.S. 3 (1883); Slaughterhouse Cases, 83 U.S. (16 Wall.)
36 (1872); Plessy v. Ferguson, 163 U.S. 537 (1896).

E.g., Helvering v. Davis, 301 U.S. 619 (1937); Korematsu v. United States, 323 U.S.

exercise federal jurisdiction over the traditionally state area of real property law) with
state area of evaluating election returns); also compare Puerto Rico Dept. of Consumer
Affairs v. Isla Petroleum Corp., 485 U.S. 495 (1988) (Scalia, for the majority, declining
to extend federal preemption to decontrol petroleum prices, based on an absence of "a
clear and manifest purpose" of Congress) with Boyle v. United Technologies Corp., 487
For this section of paper, the issue is not what the specific boundaries between state and federal power might be at any given moment in time. Rather, the point is that the boundaries are fluid, varying according to subject matter, the country's needs during a particular time period, and the inclinations of the Justices who sit on the Supreme Court. Instead of a clear gospel, there are competing principles—states' rights vs. federal supremacy, the value of experimentation\textsuperscript{111} vs. the need for uniformity.\textsuperscript{112}

Across all of this is the distinction between statutory law and common law. There is little, if any, question that state courts can create common law as they see fit, in the absence of contrary statutory provisions.\textsuperscript{113} And although there may be "no general federal common law,"\textsuperscript{114} there are numerous areas where federal courts can develop common law if they choose.\textsuperscript{115}

U.S. 500 (1988) (same term, Scalia, for the majority, extending federal preemption to cover military contracts, even without a Congressional act on point).

\textsuperscript{111} See supra note 99.

\textsuperscript{112} See, e.g., Hines v. Davidowitz, 312 U.S. 52 (1941) (relying on a need for national uniformity in immigration law).

\textsuperscript{113} Erie v. Tompkins, 304 U.S. 64, 78 (1938).

\textsuperscript{114} Id.

The basic federalist system boils down to a fluid mixture of federal, state, and municipal \textsuperscript{116} law, each of which comprises a mixture of statutory and common law. Federal law is supreme \textsuperscript{117} where the Constitution has given power to the central government \textsuperscript{118} or where the Supreme Court has found either an implied grant of power \textsuperscript{119} or an overriding need for national uniformity. \textsuperscript{120} Where federal law has not pre-empted other law, or where the federal government has explicitly granted aspects of its power to the states or municipalities, \textsuperscript{121} the state or municipality creates the law.

Within this framework, some aspects of Web law fall easily into the federal law category. For example, the Web's underlying telecommunications infrastructure is

\begin{itemize}
  \item \textsuperscript{116} "Municipal" in a domestic sense meaning town, city, and county.
  \item \textsuperscript{117} U.S. Const. art. VI.
  \item \textsuperscript{118} As in the regulation of interstate commerce. U.S. Const. art. I, § 8, cl. 3.
  \item \textsuperscript{119} E.g., dormant commerce clause. Id. See Southern Pacific Co. v. Arizona, 325 U.S. 761, 769 (1945) ("For a hundred years it has been accepted constitutional doctrine that the commerce clause, without the aid of Congressional legislation, thus affords some protection from state legislation inimical to national commerce . . ."); Railroad Co. v. Husen, 95 U.S. 465, 469 (1877) ("Whatever may be the power of a State over commerce that is completely internal, it can no more prohibit or regulate that which is inter-state than it can that which is with foreign nations.").
  \item \textsuperscript{120} E.g., immigration. Supra note 112.
  \item \textsuperscript{121} E.g., insurance regulations. 15 U.S.C. § 1012.
\end{itemize}
already regulated through federal law. Some aspects fall clearly within the realm of state or municipal law. Other aspects are less clear.

For example, if there is to be malpractice for Web site operators, the corresponding standard of care might be determined by either regional standards or central standards. Regional standards could follow the established model for medical malpractice and would logically fall under state law. Under the regional approach, though, a user accessing a Web site, when deciding how much to trust the Web site, would be unlikely to know the standard of care that applied to it, thereby making it difficult to make an informed decision about how much personal private information to share.

Central standards of care, on the other hand, could easily fit within federal law. They would offer predictability to the user and uniformity across the nation. However, they might also stifle legal innovation and overburden Web site operators in "less developed" regions.

---


123 Such as business licenses for an ISP or the zoning regulations that regulate the physical structure within which an ISP is housed.

124 E.g., for inadequately protecting personal private information that a user has shared.


125 See supra note 99.
The key point about U.S. federalism derives from its historical instability and the imprecision of the boundaries between state and federal power. The instability and imprecision yield flexibility. As Web law is far from mature, such flexibility may be particularly valuable.126

V. The Nature of Non-Governmental "Law"

Official bodies within the states, federal government, and international organizations create "law" that is binding in that government will use its power to enforce the law and coerce compliance. In a broader sense, however, "law" encompasses more than rules, regulations, and principles that the government will enforce; it also encompasses other norms, agreements, and standards that shape an individual's behavior.

126 Before concluding this brief overview of the nature of U.S. federalism, it is important to note that certain powers have also been assigned to state and federal administrative agencies. In the area of labor-management relations, for example, the National Labor Relations Board (NLRB) has been empowered to issue decisions that carry the full force of law. 29 U.S.C. § 156. In a practical sense, administrative law has a substantial impact on areas as diverse as commercial aviation, the power industry, securities, and the environment. In a structural sense, however, all of the administrative agencies derive their power from the legislatures that originally held that power. The agencies are limited in their reach to the limits of the power of the legislatures that created them. Hence, although the agencies provide an additional option for potential sources of Web law, their existence does not alter the fundamental federalist structure.
and promote a functional society. In this broader sense, non-governmental law emerges from a variety of sources, including traditions, practices, and other more or less formal agreements among groups of people.

Non-governmental law is sometimes incorporated into formal governmental law, such as when a court adopts "contemporary community standards" as part of its legal (and binding) definition of obscenity. At other times, particularly in the criminal context, the prohibition against ex post facto laws prevents retroactive governmental application of non-governmental law. With or without the power of government behind it, non-governmental law can exert substantial influence and warrants attention in any consideration of Web law.

127 Law in this sense resembles the modalities of regulation discussed by Lessig. Lessig II, supra note 13, at 86-90.


129 There is widespread disapproval of the desecration of human remains, but when the operator of a Georgia crematorium was alleged to have severely mishandled cadavers entrusted to his care, Georgia had no statute directly on point. Hence, the only crimes that he was charged with involve theft by deception. See, CNN, Crematory Operator Faces 100 New Counts, February 27, 2002, at http://www.cnn.com/2002/LAW/02/26/crematory.corpses/index.html.

130 See, e.g., Lessig II, supra note 13, at 37 (discussing differing U.S. and European norms regarding smoking).
Sources of non-governmental law can be extremely informal. "Netiquette," for example, grew out of informal consensus among early users of email and newsgroups. Similarly, multi-user online communities began by informally developing their internal norms of behavior; violations of those norms, in turn, have at times led to the development of more formal procedures.

Other sources of non-governmental law are more formal, more structured, more like quasi-governments. Part II.A of this paper, for example, discussed the IETF and W3C. These are both structured, independent organizations with central management, dues-paying memberships, and formal procedures for the development and adoption of standards.

The core work of the IETF and W3C involves the development of standard protocols; in that sense, they develop the "law" of protocols. Beyond this core work, the bodies also address issues of how things should be done, such as the IETF Netiquette FAQ or the W3C Web Content Accessibility Guidelines, which provide Web site creators with guidance for how to make their sites accessible to users with disabilities.

---

131 The polite way of using email and newsgroups.


133 See Lessig II, supra note 13, at 74-78 (describing how a multi-user community developed mechanisms of government in response to several "cyber-rapes").

134 Supra note 132.

135 Available at http://www.w3.org/TR/WAI-WEBCONTENT/.
Given their technical expertise and the fact that they have already addressed certain behavioral issues, bodies like the IETF and W3C may prove useful for developing additional, more "legal-like" standards, which might then be incorporated into more formal law, as appropriate, through reference by statute or adoption through common law.

The American Law Institute (ALI) is another potential source of law. It resembles the IETF and W3C in that it is an independent, non-governmental organization, but it differs in that its primary focus is directly on areas of law, rather than areas of the Internet or Web. ALI Restatements are, in part, useful compilations of existing law, but they also develop and suggest new directions for law to move. The ALI might therefore also have a role in the development of Web law, particularly in subject matter that requires vigorous examination of existing law. While the W3C and IETF may be well suited for developing guidelines for technical issues and general user behavior, the ALI might be a better source for guidelines regarding legal issues such as the application of bailment theory to the Web.\(^{136}\)

As Lessig points out, there is, in addition to the above non-governmental sources, the code of the Web itself—the protocols and programs that enable the Web to operate.\(^{137}\) If written one way, the code can permit certain behaviors; if written differently, the code

\(^{136}\) An additional option would be for legal organizations such as the ALI to collaborate with technical organizations such as the W3C and IETF.

\(^{137}\) Lessig II, supra note 13, at 20-21.
can constrain those behaviors.\textsuperscript{138} Such "west coast code"\textsuperscript{139} affects online behavior more directly than traditional law, in that the code proactively enables or disables capabilities rather than creating after-the-fact consequences.\textsuperscript{140}

At the same time, however, the development, implementation, and use of the code is itself subject to legal restraints.\textsuperscript{141} The code is both a source of regulation of user behavior and an object that law controls. Hence, even while exerting its own influence, the code itself is subject to the various governmental and non-governmental sources of law discussed in this paper.

\textsuperscript{138} For example, untraceable anonymity permits users to speak without fear of identification, which in turn can encourage whistle-blowers or people who wish to discuss particularly sensitive personal issues, such as AIDS or sexual abuse. See supra note 52. Code written differently, though, could eliminate the possibility of untraceable anonymity, which in turn would discourage those same discussions.

\textsuperscript{139} Lessig's phrase to distinguish it from "east coast code," the statutory code written in Washington, D.C.

\textsuperscript{140} Even an injunction is only enforced through consequences that occur after the fact of a violation of the injunction.

\textsuperscript{141} See, e.g., supra note 33 (discussing the export controls applied to encryption software); supra text accompanying note 35 (discussing the applicability of copyright law to software).
VI. A Case in Point: The CPPA

The main thesis of this paper is that the U.S. federalist system is well suited to the application of law to the Web because the system offers a diversity of legal tools to address a diversity of Web needs. Implicit in this thesis is the concept that some tools are better for certain jobs than others are. The recent U.S. Supreme Court ruling on the constitutionality of the Child Pornography Prevention Act (CPPA) demonstrates that federal statutory law, while it has its place, is not always the most appropriate source of law to use for the Web.

When an issue is "hot," legislators at the various levels of government will seek to address it by statute. In the 1980s, Texas had a state statute forbidding flag burning. In 1989, the U.S. Supreme Court found that statute to violate the First Amendment. Flag burning became a hot issue, and before the year was finished, the U.S. Congress responded with the Flag Protection Act of 1989. The following year, the Supreme Court rejected that act as well. Although Congress continues to introduce proposals to


143 Tex. Penal Code Ann. § 4209 (1989) ("A person commits an offense if he intentionally or knowingly desecrates . . . a state or national flag.").


ban flag burning, the issue no longer galvanizes public opinion to the same degree, and no proposal has passed both houses since 1989.147

As interest in flag burning has waned, interest in protecting children from the perceived dangers of the Web has waxed. In 1996, Congress passed the Communications Decency Act (CDA),148 which sought to restrict access by minors to "indecent" materials on the Web; in 1997, the Supreme Court struck down much of the CDA on First Amendment grounds.149 Also in 1996, Congress passed the Child Pornography Prevention Act (CPPA),150 which, among other things, sought to criminalize the creation, distribution, and possession of "virtual child pornography";151 in 2002, again on First Amendment grounds, the Court struck down provisions of the CPPA that did not involve actual child actors.152 In 1999, Congress adopted the Child Online Protection Act


151 In general terms, virtual child pornography involves simulated images of children. For example, computer-generated manipulations can be used to take an image of a youthful-looking adult engaged in sex and place a child's face on the adult's body.

(COPA),\textsuperscript{153} which sought to overcome the constitutional defects on the CDA; although the COPA has not yet been tested before the Supreme Court, its constitutionality is suspect.\textsuperscript{154} In each case, legislators were responding to a "hot" topic; in both of the cases decided so far, the legislators were found to have overstepped their authority.

This is not meant to suggest that Congress does not have a role in addressing Web-related issues. Among the parts of the above-mentioned acts that have survived constitutional scrutiny are the key CPPA provisions that deal with pornography that involves actual child actors.\textsuperscript{155} But in those areas where Congress' actions were struck down by the Court, the actions were not only unconstitutional but also arguably unwise\textsuperscript{156} or, from the perspective of this paper, simply an application of the wrong tool.

The CPPA ban on virtual child pornography is a case in point. Three Justices--O'Connor, Rehnquist, and Scalia--would have read the statute narrowly, restricting the interpretation of the language to "images that are virtually indistinguishable from actual


\textsuperscript{154} Lessig II, supra note 13, at 177. Ashcroft v. ACLU, 535 U.S. 564, 122 S. Ct. 1700 (2002), addressed the standards to apply to determine the constitutionality of the COPA; it did not address the underlying constitutionality itself.

\textsuperscript{155} E.g., 18 U.S.C. § 2251(c), which covers the transmission of actual child pornography by computer. The Court thereby kept the underlying rationale, based on actual exploitation of children, of New York v. Ferber, 458 U.S. 747, 756-757 (1982).

\textsuperscript{156} Lessig II, supra note 13, at 174-175.
children." A fourth Justice--Thomas--while concurring in the judgment, raised the possibility that the technology of computer-generated images might evolve to the point that "it becomes impossible to . . . prove that certain pornographic images are of real children," in which case the issue would warrant revisiting for law-enforcement reasons. The majority itself recognized that "sexual abuse of a child is a most serious crime and an act repugnant to the moral instincts of a decent people."159

This creates the backdrop of a Supreme Court that unanimously condemns the sexual abuse of a child. No Justice took issue with the prohibition against the distribution of actual child pornography. The only dissentsions regarded the boundaries of what constitutes pornography.160

The first prong for upholding the prohibition of the distribution actual child pornography came from Ferber, that actual child pornography "created a permanent record of a child's abuse, [and] . . . each new publication . . . would cause new injury to the child's reputation and emotional well-being."161 This prong, in turn, can be separated into two components: the original harm to the child and the ongoing harm to the child's

157 Free Speech Coalition, 122 S. Ct. at 1409 (O'Connor, concurring in part and dissenting in part).
158 Id. at 1406 (Thomas, concurring in judgment).
159 Id. at 1399 (majority opinion).
160 Or, in the case of Thomas, what level of proof law enforcement must meet in order to demonstrate child abuse.
161 Free Speech Coalition, 122 S. Ct. at 1401.
reputation and emotions. Even if the child him/herself does not suffer the original abuse, a "virtual image" of sufficient technical quality could cause the ongoing harm.\textsuperscript{162}

For three Justices, a "virtually indistinguishable" image would already be outside the reach of First Amendment protections.\textsuperscript{163} For a fourth, a virtual image of higher technical quality than is currently possible might fall outside the First Amendment protections.\textsuperscript{164} For the remaining Justices, one component of their rationale for not protecting actual child pornography—the ongoing harm—provides a strong argument for not protecting virtual child pornography. As technology advances, the ongoing harm component of their rationale becomes stronger.

For the current state of technology and with the broad wording of the CPPA, Free Speech Coalition was correctly decided. It does not, however, seem to be a particularly stable decision. Instead, it seems more like a holding action, a means of buying time until the issues regarding virtual child pornography can be more clearly resolved.

The defamation-like aspects of the ongoing harm to a child do not yet seem ripe for federal legislation, particularly since defamation is not traditionally an area of federal law. This seems to be an area where, if Congress would restrain itself from acting, the various states could experiment, and the various courts could evaluate detailed fact patterns, be informed by each other’s decisions, and eventually grow toward something

\textsuperscript{162} Note, however, that for virtual child pornography, based as it is on a lie, there may be state actions available for defamation and/or infliction of emotional distress.

\textsuperscript{163} Supra note 157.

\textsuperscript{164} Supra note 158.
resembling consensus. When that something resembling consensus is reached, Congress could centralize the law on the basis of experience, as opposed to simply responding to political pressure.

There are ways of developing law that exploit the strengths of the various governments and courts, and there are short cuts that lead to constitutional violations. The federal statutory ban on virtual child pornography in the CPPA was a short cut. Certain tools are better for certain jobs than other tools are: a hammer can break a board, but a saw leaves a smoother cut.

VII. Preliminary Suggestions

Even though this paper is limited in scope, it would seem incomplete without an attempt to offer some practical suggestions. The tools have been examined, their general uses described. One Supreme Court ruling has been evaluated to shed light on one tool, federal statutory law, succeeding in one application but failing in another. What is left is to suggest a few ways that the variety of tools might be usefully applied to the diversity of issues raised by the Web.

A. A Role for International Law

Given the general unwieldiness of international law, it seems a poor tool for addressing cutting-edge issues. It can, however, be a good choice for addressing large-scale issues of multinational import, particularly if new law can be based on existing international law.
As previously mentioned, international copyright law has already evolved to the point where it can, in many cases, be easily adapted to the context of the Web.\textsuperscript{165} Similar straightforward adaptations may also be available for other types of intellectual property law, including patent and trademark, at least to the extent that they have already been clarified under agreements such as the General Agreement on Tariffs and Trade (GATT).\textsuperscript{166} Copyright, patent, and trademark meet all three of the basic criteria: they are large-scale issues, they have multinational import, and they are areas where international law that can be adapted has already been developed.

Contract law can, in some instances, meet the first two criteria: it is a large-scale issue with multinational import. Contract law itself, however, does not seem to have been extensively developed at the international level. There are some contract-like issues addressed in agreements such as the North American Free Trade Agreement (NAFTA),\textsuperscript{167} but the more promising approach seems to be for parties to a contract, particularly sophisticated parties to a large contract, to continue to insert clauses that specify which municipal law will apply and which municipal court will have jurisdiction.

Beyond that, particularly for smaller transactions such as small purchases of books or music CDs, there are limits to what international law can offer. It might be possible to develop a general UN resolution for a "bill of rights" for Internet consumers. Details, though, would fall back on municipal law. To the extent that municipal law

\textsuperscript{165} Supra text accompanying notes 87-88.

\textsuperscript{166} December 15, 1993, 33 I.L.M. 1.

\textsuperscript{167} Canada-Mexico-U.S.A., December 8, 1992, 32 I.L.M. 605.
cannot practicably be enforced, law regarding small international transactions likely needs to fall back on the old principle of *caveat emptor*.

In the area of criminal law, two subjects fresh in the memory where international law might help are the use of the Internet to facilitate terrorism or the distribution of child pornography. Both have general UN resolutions to support them at the level of international law.\(^{168}\) Both, however, are rooted in physical events that occur in a geographical place—the actual terrorist act or the actual abuse of the child. Both, in turn, although frequently involving cooperation among law enforcement agencies in multiple countries, fall back onto municipal law for actual prosecutions.\(^{169}\)

This suggests a variation on the theme of international law that might have general applicability to Web law. First, a basic agreement is reached at the international level, which is true of the Berne Convention, GATT, terrorism, and child pornography, and which would be true of a general Internet consumers' bill of rights. Second, each participating country adopts internal laws to implement the basic agreement. Third, the basic agreement gives the various law enforcement agencies the ability to collaborate


\(^{169}\) See, *e.g.*, *supra* note 50.
across national boundaries. And finally, the actual litigation occurs under the local law of the country where the court with jurisdiction sits.

All of the areas suggested above involve large-scale issues with multinational import, and all except contract involve established international law that can be adapted to the Web. All can further be implemented through the pattern of general international agreements, local implementing legislation, multinational cooperation among law enforcement agencies, and final litigation under local law. They stand, then, as examples of the types of areas where the application of international law can benefit the Web.

B. A Role for Federal Law

Although state and federal law were treated concurrently in the discussion of the nature of federalism, they will now be treated separately. Concurrent treatment is helpful when discussing the philosophical and theoretical underpinnings of federalism. When discussing practical application, however, separate treatment of federal and state law becomes more helpful.

As a starting point, all federal authority is limited by the U.S. Constitution, as interpreted by the U.S. Supreme Court. Regardless of how beneficial federal law might be for a particular subject, unless it falls within the fluctuating outer boundaries set by interpretation of the Constitution, it is not valid and cannot be used.

A second constraint is that the Constitution grants a potential for power, but until that power is exercised by Congress, both the courts and the executive branch are

\[170\] Supra Part IV.
generally prohibited from exercising it.\textsuperscript{171} For the purposes of this paper, this constraint 
primarily affects the exercise of federal common law by the courts. By its very nature, the 
Web involves interstate and international communications, all including a commercial 
component.\textsuperscript{172} Web regulation is easily brought within the broad parameters of the 
interstate commerce clause.\textsuperscript{173} Hence, the scope of regulation that Congress could 
theoretically impose on the Web is extremely large.\textsuperscript{174}

The federal courts, however, cannot exercise federal common law over the entire 
Web; they are limited to the regions of law, or closely related regions, that Congress has 
addressed. For example, federal common law can address the interstices in the federal 
civil causes of action related to hacking into protected computers,\textsuperscript{175} but federal common 
law cannot extend such civil causes of action beyond those specifically provided for by 
statute.

\textsuperscript{171} One exception to this general statement involves the areas that are unambiguously and 
exclusively assigned to the federal government, such as the power to make treaties. \textit{U.S. Const.} art. 2, § 2.

\textsuperscript{172} Even a "free" Web site is built upon a series of commercial transactions, many of 
which are interstate in character, ranging from the construction of the various computers 
to the provision of the communications links.

\textsuperscript{173} \textit{U.S. Const.} art. 1, § 8.

\textsuperscript{174} At least within national boundaries.

\textsuperscript{175} 18 \textit{U.S.C.} § 1030(g) provides for a federal civil cause of action \textit{under the section only} 
if one of six specific factors is met.
Within these constraints, there are numerous areas where federal law might be useful for the Web. First, federal law is necessary in areas where Congress has already preempted state power. Second, federal law is useful in areas where national conformity in law is valued.\textsuperscript{176} Third, federal law is necessary in those areas over which the Constitution has given exclusive power to the federal government. And finally, federal law will tend to be more reasonable if a national consensus has already emerged about what reasonable law would be, not infrequently through permitting the states to perform their process of experimentation for long enough for a consensus to ripen.

Examples of areas where Congress has already exercised power include the regulation of the telecommunications infrastructure underlying the Web\textsuperscript{177} and the criminalization of hacking into federally protected computers\textsuperscript{178} or using the Web to distribute actual child pornography.\textsuperscript{179} A less obvious example involves employment practices. No one had the Web in mind when originally developing federal law regulating employment practices.\textsuperscript{180} But the Web can be used to establish employment contracts, various types of work can be performed across the Web, and any type of work product that can be fixed in electronic media can be transmitted across the Web. Hence, if an

\textsuperscript{176} By analogy to immigration law and treaty implementations. See supra notes 112 and 64.

\textsuperscript{177} Supra note 122.

\textsuperscript{178} Infra note 207.

\textsuperscript{179} Supra note 155.

employment relationship would otherwise be covered by federal law in a non-electronic environment, and if the only variation on that relationship is that it is Web based, then the same federal law will still apply to the Web. Congress historically exercising power in a non-electronic environment thereby creates an exercise of power over a region of the emerging electronic environment. Along with the exercise of power comes the pre-Web federal common law that was developed to fill the interstices in statutory law.181

Beyond the areas where federal law has in fact already preempted state law, there are areas where new federal law can be useful to promote the goal of national consistency. Sometimes national consistency is compelled by practical considerations.182 At other times, though not compelled, national consistency becomes desirable as a reflection of an emerging national consensus.183

181 This follows the pattern established in Textile Workers Union v. Lincoln Mills, 353 U.S. 448 (1957).


183 In this context, the Civil Rights Act of 1964, 88 Pub. L. 352, 78 Stat. 253, can be viewed as the larger part of the nation imposing its emerging consensus regarding race relations upon a dissenting region of the nation. Similarly, the CPPA prohibition against using the Web to distribute actual child pornography is an instance of federal law reflecting national consensus. The suppression of child pornography is not necessary for the government to function effectively, but consensus condemns child pornography. The
A promising area of federal work, based upon an emerging national consensus, involves federal protection of privacy on the Web. Privacy is often referred to as a "right," but there is no express right of privacy in the Constitution. The various Supreme Court decisions that have found something resembling a right to privacy have been less than thorough in their explanation of its source and parameters. Still, there is a broad expectation of privacy among U.S. citizens and a general perception that it is a right. 

dispute regarding virtual child pornography, conversely, reflects a lack of consensus about what the reach of the prohibition should be. 

The popular formulation of privacy being part of a "penumbra" of constitutional rights, Griswold v. Connecticut, 381 U.S. 479, 483 (1965), has since been abandoned by the Court. Roe v. Wade, 410 U.S. 113, 152-153 (1973) (A "penumbra" of statutory protections, however, seems to remain. Complete Auto Transit, Inc., v. Reis, 451 U.S. 401, 406 (1981).) Current thinking seems to root privacy in "the Fourteenth Amendment's concept of personal liberty and restrictions upon state action," Roe, 410 U.S. at 153, though that approach suffers from the limitations that the 14th Amendment extends only to state actions, that 5th Amendment due process-based equal protection against federal actions is implied rather than express, and that neither the 14th nor the 5th Amendment provides protection against private actions. This author personally believes that the root of the right can be found among the unenumerated rights of the 9th Amendment and the rights reserved to the people in the 10th Amendment. Whatever its roots, and whatever its validity as an actual Constitutional right, privacy is an expectation of the U.S. populace that has become so valued that it resembles a Constitutional right. It is "right-like."
Given the consensus that privacy should be protected and the fact that the federal government has the authority to regulate the Web, the protection of privacy is an area where federal law is a good tool to apply to the Web. The federal government has responded with several initiatives, leading, for example, to a series of informative reports. Congress, in its turn, has enacted limited protections in legislation such as the Electronic Communications Privacy Act (ECPA) and the COPA. These acts do not

Regardless of the independent status of privacy as a right, however, Congress, under the interstate commerce clause, has ample power to protect it against any actors, governmental or private, who might intrude into it.

Cf. Winston S. Churchill, A History of the English Speaking People: The Birth of Britain 60 (Dodd, Mead & Co. 1958) (Of King Arthur: "It is all true, or it ought to be; and more and better besides.").


yet reach issues such as Web sites that collect semi-sensitive personal information and then pass that information on to marketing firms, but the federal action to date is a promising move toward a more thorough protection of privacy. Such protection would serve the goal of national consistency and reflect a general consensus.

Another area where federal law might be useful is contracts. Although contracts, per se, generally fall under state law, interstate contracts fall within the potential power of the interstate commerce clause. Law for Web-based contracts would benefit from national uniformity, in that both consumers and providers would have more consistent expectations. Furthermore, the Uniform Commercial Code has been widely enough adopted by the various states that a large area of consensus has emerged.

In the area of Web contracts, federal law should not attempt to be overly comprehensive. Too much detail would lead to competing and potentially conflicting bodies of law—one federal for Web contracts, the other state for non-Web contracts.


189 Such as email addresses and phone numbers.

190 At least among users of the Web, if not among those who seek to profit by the sale of others' personal information.

191 For example, the Uniform Commercial Code Locator at Cornell University links to statutes from 49 states and the District of Columbia that correspond to UCC Article 1. At http://www.law.cornell.edu/uniform/ucc.html.
which could in turn lead to all of the difficulties created by Swift v. Tyson.\textsuperscript{192} This factor counsels restraint and a certain generality about federal contract law.

Nor should federal law interfere with the ability of sophisticated parties on a relatively equal footing to choose the law that should govern large-scale contracts. Choice of law is one of the issues that such parties negotiate, and as their agreed upon choice is factored into the value and expectations of the contract, so should their choice be respected. This consideration counsels a federal focus on small-scale transactions where one of the parties may be less sophisticated than the other.

The result of these considerations parallels the suggestion for potential international law: a bill of rights for Web consumers. If an international bill of rights could be established quickly enough, the federal law could be used to implement it consistently throughout the states. Otherwise, a consistent federal law might provide both an interim continuity among the states and a basis for future international negotiations. Either way, a general federal law would provide the benefit of national uniformity without interfering with the states' ability to experiment with the details.\textsuperscript{193}


\textsuperscript{193} If general federal statutory contract law for the Web were established, the ability of the states to continue to experiment with the details would rely on the wording and construction of a saving clause within that legislation. In Pilot Life Insurance Co. v. Dedeaux, 481 U.S. 41 (1987), for example, the Supreme Court found that the saving clause in ERISA, 29 U.S.C. § 1144(b)(2)(A), was insufficient to preserve a state action for improper processing of disability claims. The power of the courts to extend federal
Federal law might also be helpful in addressing tort negligence on the Web. Admittedly, torts are traditionally an area left to the states, and the bulk of the body of tort law that currently exists was developed by the states. Furthermore, no consensus about the issue seems to have emerged. Indeed, except for a few academic articles, the question of whether tort negligence can even be applied in a Web context has barely been discussed.

Nevertheless, the potential benefits of addressing negligence at the federal level are compelling. Users would have a consistent set of expectations, and providers would know what was expected of them. When an unintentional harm occurred, the victim, the tortfeasor, and the courts would all be spared the complexities of choosing among preemption even in the face of a saving clause suggests that any such clause in a federal statute for Web contracts must be explicit and unequivocal in its preservation of state powers.

Negligence could address either the failure to adequately protect sensitive information, supra note 117, or the failure to adequately protect a computer from hacking, thereby enabling others to use it as a base for attacks against other computers. See, e.g., Stephen E. Henderson & Matthew & Yarbrough, Suing the Insecure?: A Duty of Care in Cyberspace, 32 New Mexico Law Review 11 (2002); David L. Gripman, The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem, 16 J. Marshall J. Computer & Info. L. 167 (1997).

Supra note 194.
competing bodies of law. A single law would apply, at least within national boundaries. Consistent expectations would then promote better informed behaviors on the part of both users and providers.

Such law could be constructed in a manner that would permit flexibility in the face of technological evolution. A general statute could federalize the issue of tort negligence for ISPs. The definition of a reasonable standard of care could be left to subject matter experts (SMEs) such as the W3C. The proper application of the combination of federal statute and SME standards could be left to federal common law.196

The above examples illustrate areas where federal law has already addressed Web issues with success and areas where federal law holds promise for the Web issues. There remain, however, the constraints. Federal statutory law cannot exceed the broad limits set by the Constitution, and federal common law cannot exceed the narrower limits of the scope of power that Congress has chosen to exercise.197 Within these constraints, it is generally preferable to restrict federal law to areas where a national consensus has emerged,198 though at times the value of national consistency overrides the desirability of consensus.199

196 This specific approach to federalizing tort negligence for ISPs by combining law from various sources is discussed in more detail in Part VII.E of this paper.

197 The Constitution defines the limits of the field; Congressional action determines how much of that field the federal government has occupied.

198 See, e.g., supra note 183 and accompanying text.

199 See, e.g., supra text following note 195.
C. A Role for State Law

Given the plenary nature of state power, state law should be applied to all areas that require formal, governmental law and that have not yet been addressed by international or federal law. The inclusionary aspect of this formulation—all areas that require formal, governmental law—encompasses areas of law that have traditionally been within state power, unsettled areas that could benefit from experimentation, and whatever other areas that might fall into the gaps within existing law. The exclusionary aspect of this formulation has already been addressed in the two preceding sections of this paper.

This paper has already suggested that state law is the appropriate tool for addressing virtual child pornography. Any state treatment of this issue will be subject to the same First Amendment constraints as were applied in Ashcroft v. Free Speech Coalition. The constitutional flaw that the majority found in that case was that the particular wording in the CPPA regarding virtual child pornography was overbroad. The key to overcoming that deficiency is to develop wording that is sufficiently narrow to meet the First Amendment requirements. An ideal way to develop that wording would be

---

200 The inclusionary aspect itself contains an exclusionary element—the need for governmental law to be required. Any formal law will only cause disruption if it is extended into areas where it is not needed, such as, for example, the detailed specification of technical protocols.

through experimentation—multiple states enacting multiple statutes with multiple variations of wording, each of which can in turn be tested by various courts.²⁰²

State law should also address any issues related to hacking²⁰³ into individual users' computers that federal law has not specifically preempted. Logically, an individual's computer is a form of personal property. When that computer is linked to the Web, its resources become a "site" within the Web, leading to a cyber-variant of real property.²⁰⁴ These analogies lead to unauthorized access to a computer being a form of trespass²⁰⁵ and unauthorized use of a computer being a form of conversion.²⁰⁶ Both

²⁰² In addition to statutory criminal law, the states can explore the civil tort of defamation as a potential path for developing the formulation of law that would be held constitutional.

²⁰³ "Hacking" here is used in a broad sense to include both active attacks, where the hacker is interactively seeking unauthorized access to a computer, and passive attacks, where the hacker sends out a virus or worm that automatically gains access and replicates itself.

²⁰⁴ Geocities, following this analogy, previously referred to those who create Web pages on its computers as "homesteaders."

²⁰⁵ An alternate path to reach the same conclusion is to view unauthorized access as trespass to chattels. See, e.g., AOL v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000) (finding that, under Virginia common law, trespass to chattels can be applied to unauthorized access to computer systems).

²⁰⁶ See, e.g., id. (blending conversion into the trespass to chattels analysis).
trespass and conversion are traditional areas of state law, and because of the relative newness of applying them to the Web, trespass and conversion are good candidates for state experimentation.

The federal Computer Fraud and Abuse Act (CFAA), as revised, is extremely expansive in scope in terms of the computers it covers. With language extending its protections to any computer "used in interstate or foreign commerce or communication," the CFAA can be read to cover any computer that connects to the Web. The types of unauthorized access and use that it criminalizes are, however, specifically defined, and the CFAA contains no preemption clause. Absent express preemption, state law remains intact insofar as it does not directly contradict the federal law. States are therefore free to complement the CFAA protections through state statutory and common law.

---


209 See, e.g., Allis-Chalmers Corp. v. Lueck, 471 U.S. 202, 208 (1985) (where the threshold question was whether Congress intended preemption). The requirement that state law not contradict the federal law is due to the supremacy clause. States can supplement federal prohibitions, but they cannot constitutionally legalize a federally proscribed activity.

210 See, e.g., National Health Care Discount, 121 F. Supp. 2d at 1271-1276, 1276-1277, 1277-1279 (allowing AOL's claims to proceed to trial concurrently under the CFAA, Virginia statute, and Virginia common law, respectively).
Although this paper argues that tort negligence by ISPs should be a federal issue, many other civil causes of action remain better left to the states. Trespass and conversion have already been addressed; other examples include defamation, infliction of emotional distress, and loss of consortium. All are traditionally areas of state law; none, in the context of the Web, have a compelling need for national consistency or a clear national consensus. In addition, as this paper has already argued, state law seems the best choice for resolving the details of contract law in the Web context.

---

211 Supra Part VII.B.

212 One exception to the lack of a need for national consistency is that all state law remains subject to the constraints of the Constitution. Defamation law, for example, regardless of whether it is used in a Web context, remains constrained by the First Amendment. See, e.g., Hustler Magazine v. Falwell, 485 U.S. 46 (1988).

213 In addition, several of the torts that this paper argues should be left to the states—trespass, conversion, and defamation, in particular—involve intentional tortfeasors. The operation of law has numerous inherent biases in favor of one party or another, such as presumptions in choice of forum or choice of law. In general, the greater the tortfeasor's intent, the more those biases should be shifted in favor of the victim. An unintentionally negligent ISP is more entitled to biases such as consistent national standards of care, since potential exposure to varying standards of care will tend to suppress the ISP's willingness to participate in the Web. An intentional hacker, however, is less entitled to biases in his/her favor, since knowingly causing harm is less deserving of protection than unknowingly permitting harm to occur. The victim of an intentional tortfeasor should
Even with the broad formulation that state law should be applied too all areas that require formal, governmental law and that have not yet been addressed by federal or international law, there is still the restriction that formal law be required. The examples given above are all areas where formal law steps in when more or less informal self-regulation fails. There remain, however, areas where the Web should be left unconstrained by any governmental law.

D. A Role for Non-Governmental Law

Non-governmental "law" can cover all areas that do not require a governmental power to enforce. This includes, in fact, the vast majority of technical issues and user behavior. While deliberate defamation is a subject where formal law is, at times, appropriate, inadvertent spamming is better left to informal mechanisms such as user education.

In addition to the constitutional and structural constraints on formal law discussed in previous sections of this paper, there are certain practical constraints. For one, lawsuits are expensive. Even if formal law creates a right, it would not be affordable for an individual to bring a formal suit to enforce that right unless the harm were significant

therefore be more entitled to whatever advantages can be found in choice of forum, choice among various states' law, and other sources of bias.

214 Supra Part VII.B.

215 See, e.g., supra note 103, text following note 210.

216 Such as when an email user accidentally responds to all rather than simply responding to the sender.
enough. For small harms where suits are impracticable, non-governmental mechanisms are the appropriate tool for protecting individuals' interests.

A second practical constraint on governmental law is that the various officials who make such law are not generally experts in the technical side of the Web. Legislators and judges are not the right groups to be debating the relative merits of assigning different meanings to the second four bits in an Internet Protocol version 6 packet. Such technical issues are best left to the organizations of SMEs that specialize in developing the technical specifications, such as the IETF and W3C.

---

217 Similarly, a class action based on small harms would not practicably be brought unless a sufficient number of individuals suffered similar harms.

218 For example, if a member of a newsgroup misuses that group by posting inappropriate messages, the manager of the newsgroup can protect the group's interests by removing the individual's permission to post messages to the group.


220 The government does sponsor groups such as the National Institute of Science and Technology (NIST) that develop technical specifications that are applicable to the Web. See, e.g., Advanced Encryption Standard Home Page at http://csrc.nist.gov/encryption/aes/. Specifications from these groups are governmental, in the sense that government sponsors the groups. The specifications are not, however, formal law, in that adherence by non-federal groups is voluntary.
An additional practical constraint on governmental law is that it tends to evolve slowly. Statutory law can take years to develop.\textsuperscript{221} Common law does not develop until a suit is brought and decided, and the common law does not become final for \textit{stare decisis} purposes until the suit has been appealed to, accepted by, and decided by the highest court for the subject matter.\textsuperscript{222}

As a result of this slowness of governmental law, issues whose solutions need to evolve quickly should be left to non-governmental sources. One example already discussed in this paper is the specific issue of a reasonable standard of care for ISPs in protecting sensitive information.\textsuperscript{223} Another example lies in encouraging organizations such as the ALI to collaborate with SMEs in adapting existing documents such as Restatements to the Web.\textsuperscript{224}


\textsuperscript{222} The U.S. Supreme Court for federal issues, state supreme courts for state issues.

\textsuperscript{223} See, supra, text accompanying note 196.

\textsuperscript{224} Adapting existing documents to the Web seems preferable to any attempt to develop a separate body of Web law. For example, the fundamental elements of a contract remain the same regardless of whether it is executed face-to-face, through the mail, or online. It
Within this general framework, non-governmental entities need to realize that, if they do not effectively address issues that matter to users, there will be increased pressure for governmental agencies to intervene and apply formal law. To the degree that non-governmental entities fail to counter offensive or abusive online behavior, there will be motivation for the government to intrude. Hence, a warning: to the extent that the Web community does not wish to be constrained by formal law, it must self-regulate.

E. A Role for Hybrids

A common thread running through many of the above examples is the idea that Web law might benefit from the integrated application of different types of law. International law can condemn child pornography; federal law can criminalize actual child pornography; and the states can experiment with approaches to virtual child pornography. A general Internet consumers' bill of rights can be established at the international or federal level, and the states can fill in the details.

A promising area for the application of such hybridized, integrated law lies in tort negligence for ISPs. On the one hand, there are strong reasons to have nationally uniform law, including consistency of expectations among users and a consistent understanding of duty among providers. Legislatures and courts, however, are not well suited to evaluating the technical details of a particular Web site's security configuration.

therefore seems that the bulk of the extension of existing secondary sources to address the Web can be handled through revised commentary, rather than through revisions to the underlying rules.
A hybridized approach could begin with a federal statute that federalized the general issue of tort negligence for ISPs and preempted states from addressing the issue. Details, such as the definition of a reasonable standard of care, would be incorporated, by reference, from work products of SMEs such as the W3C. As the SMEs revised their standards to reflect technological change, so would the federal law evolve, without the need for additional action by Congress. The mechanisms for applying the combination of federal statute and SME standards could be left to federal common law. Consistency would come from the federalization of the issue, flexibility would come from the delegation of details to the SMEs, and practicality would come from the courts deciding the controversies that arose on a fact-specific basis.

The mixture of different levels of detail from different sources of law adds to the overall flexibility of the U.S. federalist system. By increasing the flexibility, the possibility of mixing law from different sources can only add to the potential effectiveness of the application of law to the Web.

VIII. Summary

The U.S. federalist scheme is flexible enough to accommodate law from multiple sources, including international, state and federal, and non-governmental sources. The

---

225 Subject to Learned Hand's warning that, if the industry's standards should lag too far behind reasonable expectations, it is the role of the courts to impose higher standards. The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("Courts must in the end say what is required . . .").
boundaries between these sources are fluid. Yesterday's customary practice can become today's state common law, which can in turn become tomorrow's federal statutory law.

The Web itself is young, and the legal issues it raises are diverse. Although certain issues fit relatively neatly under existing law, other issues can find nothing more direct than a rough analogy. The diversity and newness of issues, when combined with the fluidity and flexibility of the U.S. federalist system, compels the conclusion that the federalist system has the potential to be particularly well suited to the application of law to the Web. Along with the potential, the mix creates the challenge to best use the toolbox of the federalist system to develop good, effective law for the Web. When the

---

226 With "relatively" being a key word. For example, copyright is easy when one person copies another person's work and posts it on his/her Web site. WebbWorld, supra note 54. It becomes more complicated, though, when the copying user incorporates the creating user's content via a hyperlink. Kelly v. Arriba Soft Corp., 280 F.3d 934, 938 (9th Cir. 2002). The potential for such complexity is increased by the Web's trend toward more fine-tuned identification of online material. See, e.g., RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax, § 1.2 URI, URL, and URN (IETF RFC, 1998), available at http://www.ietf.org/rfc/rfc2396.txt.

227 Such as the analogy to medicine for malpractice for Web site operators. Supra text following note 124.
potential benefits of a well implemented Web are added to the mix, the challenge becomes a near-moral imperative.\textsuperscript{228}

\textsuperscript{228} Cf. Luke 12:48 ("For unto whomsoever much is given, of him shall much be required.").