Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace

David G. Post
David.Post@chicagounbound.edu

Follow this and additional works at: http://chicagounbound.uchicago.edu/uclf

Recommended Citation

This Article is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
Crime on the Internet also presents the critical issue of anonymity. ... The development of secure, anonymous electronic mail will greatly impair the ability of law enforcement to track terrorist communications. For example, one Internet posting regarding the Oklahoma City bombing and bomb construction was sent through an "anonymous remailer"—a device designed to forward electronic mail so that the original sender is unknown—probably to prevent tracing. ... Although prior communication methods permit anonymous communications, those services generally provide one-to-one communications. It would be both time-consuming and costly to use either the phone or mail systems to disseminate information wholesale, [which] effectively prevent[s] wide-scale malicious use and limit[s] the harm that can be caused. On the Internet, by contrast, there are no monetary or technical impediments to worldwide dissemination of communications. Anonymous, worldwide dissemination of terrorist information must be of paramount concern to law enforcement and to ordinary citizens.¹

¹ Visiting Associate Professor of Law, Georgetown University Law Center, and Co-director, Cyberspace Law Institute. E-mail: Postd@law.georgetown.edu or david.post@counsel.com. My thanks to David Johnson, Mark Lemley, Michael Froomkin, and the pseudonymously named "Perry the Cynic," for comments on earlier formulations of the ideas presented here, as well as to the participants on the Cyberia-L listserv generally for their contributions to my thinking on these questions. As is customary, I bear all responsibility for the manner in which those ideas are expressed.

¹ Hearings on "Mayhem Manuals and the Internet" before the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee, 1995 WL 293484 (FDCH) (May 11, 1995) (Testimony of Robert S. Litt, Deputy Assistant Attorney General, Department of Justice, Criminal Division).
Over the past year or two, the ease with which individuals can communicate anonymously in cyberspace has begun to sink into our collective consciousness. Enormous quantities of information about the activities of anonymous remailers are now freely available, and discussions about the implications of widespread anonymity have become commonplace in the popular press as well as, increasingly, in scholarly literature. Calls for

2 I use the term "cyberspace" here to mean the global aggregate of digital, interactive, electronic communication networks; cyberspace thus includes the constituent networks comprising the global internetwork (the "Internet"), as well as the Internet itself as a separate, emergent phenomenon. A number of "technologies" are excluded intentionally from this definition: for example, noninteractive media (current television-broadcasting and cable-network systems), or nonnetworked computer applications (a videogame, for example, or a computerized spreadsheet). Similarly, although one can imagine an analog interactive network—indeed, one doesn't need to imagine such a network, for the worldwide telephone network provides a good example—that, too, is not, for my purposes, part of cyberspace. These exclusions are intentional; for reasons explored in more detail in David R. Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace (forthcoming, Stan L Rev) (1996) (unpublished manuscript on file with the University of Chicago Legal Forum), this definition captures those distinctive characteristics of the new "place" that, taken as a whole, have the most substantial effect on the applicable laws governing conduct within the medium.

3 Only a short while ago, Hardy, in his pioneering discussion of law in cyberspace, could write that "allegedly anonymous remailer computers on the Internet exist in Finland, for example," citing a personal conversation with Mike Godwin, counsel for the Electronic Frontier Foundation. I. Trotter Hardy, The Proper Legal Regime for "Cyberspace", 55 U Pitt L Rev 993, 1011 n 45 (1994).

4 A wealth of information about anonymous remailers can be found online at http://www.cs.berkeley.edu/~raph/remailer-list.html; http://www.cs.berkeley.edu/~raph/remailer-FAQ.html; http://www.well.com/user/abacard/remail/html; http://electron.rutgers.edu/~gambino/anon_servers/anon.html; http://chaos.taylored.com:1000/1/Anonymous-Mail. Information about one of the more prominent remailers, the anon.pen.et.fi service, can be obtained by electronic mail at info@anon.pen.et.fi. See, generally, A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases 7-12 (Paper presented September 21, 1995, at the Conference for the Second Century of the University of Pittsburgh School of Law) (unpublished manuscript on file with the University of Chicago Legal Forum) (available online at http://www.law.miami.edu).

5 See, for example, Charles Arthur, Pornographers on Internet Skilled at Covering Tracks: Network Impossible to Censor, Independent 3 (July 27, 1995) (discussing the "enormously difficult task" of tracking down pedophiles who "can use 'anonymous remailers'—computers which receive messages and strip off the details of their sender, before forwarding it elsewhere on the network"); Douglas Lavin, Anonymous Service an Internet Loophole: As Governments Try to Limit Content, Global Resistance Grows, San Diego Union-Tribune 7 (July 25, 1995) (discussing the anon.pen.et.fi anonymous remailer service, the "electronic-publishing equivalent of offshore banking"); Chip Rowe, Censorship Glossary: Pertaining to Computer Online Services, Playboy 48 (July 1995) (describing anonymous remailers); Helen Nowicka, Innovations: Vice Squad Cleans up the Superhighway, Daily Telegraph 16 (June 27, 1995) (describing discovery by West Midlands vice unit that "[c]hild pornographers conceal their actions by sending encrypted images, or having their electronic address removed by an anonymous remailer"); Charles Arthur, Super
some form of state regulation of anonymity in cyberspace are on the rise, and this, in turn, will prompt increased public debate.


Opening the Senate hearings on "Mayhem Manuals and the Internet," Senator Arlen Specter remarked:

Among those who communicate on the Internet are purveyors of hate and violence. Among the full text offerings on the Internet are detailed instruction books describing how to manufacture a bomb. The most widely known manual is the "Big Book of Mischief." This 93-page document details explosives formulas, how to purchase explosives and propellants, and how to use them.... Anyone with access to the Internet can obtain this recipe for disaster, even a 10-year-old child who can find a glass container and some gasoline.... There are also electronic mail discussion groups where information on bomb making can be traded anonymously. One disgusting example is this anonymous message posted on an Internet electronic bulletin board shortly after the Oklahoma City bombing: "Are you interested in receiving information detailing the components and materials needed to construct a bomb identical to the one used in Oklahoma? The information specifically details the construction, deployment, and detonation of high powered explosives. It also includes complete details of the bomb used in Oklahoma City, and how it was used and how it could have been better." The individual who posted this message, who cowers in anonymity, deserves condemnation for using the Internet to suggest how the Oklahoma City bombing "could have been better." This is just one of many other examples.... Among the issues before us are the extent of such usage of the Internet and whether anything can or should be done to curb it.


Similarly, Section 502 of the recently enacted Telecommunications Act of 1996, amending 47 USC § 233, makes it a federal crime for anyone to "utilize[ ] a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications." Communications Decency Act of 1996, Pub L No 104-104, 110 Stat 56 (1996), to be codified at 47 USC § 223 (emphasis added).
about the costs and benefits associated with anonymous communication.

At least in the rather unusual circumstances of cyberspace, that debate must pay particularly close attention to anonymity's close cousin, pseudonymity. On the one hand, it will be difficult, and at times impossible, to distinguish pseudonymous and anonymous messages from one another; as a result, attempts to restrict or eliminate anonymous speech will a fortiori have an effect, intended or otherwise, on the availability of pseudonymous messaging as well. The costs and benefits associated with pseudonymity must therefore be part of the overall equation for assessing the wisdom of alternative schemes for regulating anonymous speech. But the benefits of pseudonymous speech may be quite far-ranging and quite distinct from the benefits normally associated with anonymous-messaging systems. Pseudonymous speech is valuable in a way that anonymous speech is not and cannot be, because it permits the accumulation of reputational capital and "goodwill" over time in the pseudonym itself, while simultaneously serving as a liability limitation insulating the speaker's "true identity" from exposure. Using liability limitations as a mechanism to foster a particular goal—the formation of collective enterprises capable of accumulating reputational capital—is a device familiar from the corporate law context, and it is my contention that pseudonymous speech is capable of playing a similar role in cyberspace. The debate over the proper scope of anonymity regulation therefore needs to be broadened to take this feature of pseudonymous speech expressly into account.

I. ANONYMITY AND THE LAW

The framework for the anonymity debate appears reasonably well settled. On the cost side of the ledger, anonymous messaging makes it impossible for "law enforcement"—broadly defined to include both public and private enforcement mechanisms—to obtain information about, and thus pursue legal action against, the person or persons responsible for harmful behavior. There is also the attendant moral-hazard problem: to the extent individuals can avoid internalizing the costs that their behavior imposes on others, widespread anonymity may increase the aggregate amount of harmful behavior itself.  

---

8 See, for example, Ann Wells Branscomb, Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace, 104 Yale L J 1639, 1642 (1995) (cited in
On the benefit side of the balance, as the Supreme Court noted some time ago, "[i]t is plain that anonymity has sometimes been assumed for the most constructive purposes." There are perfectly legitimate—laudable, even—reasons why individuals might want to engage in communicative activity without disclosing their identities, and profound public benefit that may be derived from allowing them to do so. By permitting individuals to communicate without fear of compromising their personal privacy and without fear of retribution, anonymity permits information to be injected into public discourse that might otherwise remain undisclosed—information about the views of political dissenters, for example, or "whistleblower" information that may help uncover the existence of illegal activity.\(^9\)

---

\(^9\) Talley v California, 362 US 60, 65 (1960).

\(^10\) See, for example, Branscomb, 104 Yale L J at 1642 (cited in note 6) ("There are numerous situations in which anonymity seems entirely appropriate and even desirable. Psychologists and sociologists point out that people benefit from being able to assume different personae. It is therefore natural that individuals use electronic communication to disguise themselves, as in costume balls in the multiuser dungeons (MUDs) that Howard Rheingold describes.... The media often cite 'a prominent source' who does not wish to be identified, and pseudonymous authors have long been with us, sometimes in the past to prevent disclosure that the writer was female for fear her work would not be published were her gender known.... Anonymity has also been protected in cases in which actual retaliation or harm may ensue if the source of the writing is known, as in the case of whistle-blowers or political dissidents under authoritarian regimes.") (citing Howard Rheingold, The Virtual Community 145-50 (Addison-Wesley Publishing Co., 1993); Froomkin, Flood Control at 23 (cited in note 4) ("Anonymous electronic communication greatly enhances the privacy of the author. This is a good to the extent that privacy itself is a good, and while privacy may be a good, it is not wholly good or costless."); Comment, 55 U Pitt L Rev at 1178 (cited in note 6) ("Abused as a child, an adult decides to share his story with a support group. A young woman who has tested positive for HIV discusses her feelings with others affected by the AIDS virus. After observing illegal activities at his
This framework is undoubtedly a useful one, and these considerations are indeed necessary ingredients of any discussion about regulating anonymity in cyberspace. I do not intend my discussion to replace, or to repeat, this analysis. Instead, I want to inject a new set of concerns into this ongoing debate. I want to suggest that an analysis of anonymity in the rather unusual circumstances of cyberspace brings a new suite of costs and benefits into play that have, perhaps, received little attention up to now (at least in this context), and that therefore the existing analytical framework must expand to take these concerns into account.

New approaches to the problem of anonymity in cyberspace will certainly be needed if only because there is not really any existing law regarding truly anonymous communications or transactions, for the simple reason that such communications or transactions are, by definition—because the responsible party is unknown—beyond the reach of ordinary legal processes. Consider, by way of illustration, the facts in McIntyre v Ohio Elections Commission, the Supreme Court’s most recent brush with the legal issues surrounding the regulation of “anonymous” communication. Mrs. McIntyre distributed leaflets to persons attending a public meeting at the Blendon Middle School in Westerville, Ohio, expressing opposition to a proposed school tax levy. Some of the leaflets she distributed identified her as the author; others merely indicated that they expressed the views of “Concerned Parents and Taxpayers.” The Ohio Elections Committee fined Mrs. McIntyre one hundred dollars for violating the relevant statute, which provided that:

No person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to . . . promote the adoption or defeat of any issue . . . through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication...
in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefor.\textsuperscript{13}

The Court described the issue in the case as "whether an Ohio statute that prohibits the distribution of anonymous campaign literature is a 'law . . . abridging the freedom of speech' within the meaning of the First Amendment."\textsuperscript{14} In the course of its opinion, the Court discussed—at times eloquently—the "important role in the progress of mankind" that "[a]nonymous pamphlets, leaflets, brochures and even books have played."\textsuperscript{15}

Anonymity . . . provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent. Thus, even in the field of political rhetoric, where the identity of the speaker is an important component of many attempts to persuade, the most effective advocates have sometimes opted for anonymity. [There is] a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation.\textsuperscript{16}

The Court concluded:

Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in

\textsuperscript{13} Ohio Rev Code Ann § 53599.09(A) (Banks-Baldwin, 1988), excerpted in McIntyre, 115 S Ct at 1514-15 n 3 (emphasis added).

\textsuperscript{14} McIntyre, 115 S Ct at 1514.

\textsuperscript{15} Id at 1516 (quoting Talley, 362 US at 64).

\textsuperscript{16} McIntyre, 115 S Ct at 1517 (internal quotations and footnotes omitted).
general, our society accords greater weight to the value of free speech than to the dangers of its misuse. Ohio has not shown that its interest in preventing the misuse of anonymous election-related speech justifies a prohibition of all uses of that speech.\(^\text{17}\)

But in what sense was "anonymity" the issue in this case? The Ohio statute indeed "prohibit[ed] the distribution of anonymous campaign literature."\(^\text{18}\) The actions that led to Mrs. McIntyre's punishment, however, were not anonymous at all—she went to a meeting of her neighbors and, acting in a manner such that her identity was evident to all, distributed a certain category of campaign literature; that is, literature without printed identification. There were, on reflection, two elements to the offense with which Mrs. McIntyre was charged: (1) anonymous communication (through a "notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to . . . promote the adoption or defeat of any issue")\(^\text{19}\); and (2) some nonanonymous action sufficient to allow her to be identified and charged with the offense. Both were required elements, but only with respect to the first did the Ohio legislature make a choice; the second is a consequence of a more fundamental requirement that rules can only be enforced by identifying some party against whom to proceed.

Both the presence and the absence of anonymity were thus necessary preconditions to enforcement of the Ohio statute. This is a bit odd, but it is little more than a theoretical oddity in a world—such as the one the Ohio legislators surely had in mind—where perfect anonymity is difficult to achieve and where the absence of perfect anonymity can, generally speaking, be counted on to resolve the enforcement dilemma.\(^\text{20}\) But cyberspace is not such a world.

\(^{17}\) Id at 1524 (citations omitted).


\(^{19}\) Id.

\(^{20}\) In the nonvirtual world, to have achieved truly anonymous action Mrs. McIntyre would have had to go to considerable trouble and expense. At the very least, she would have required her own printer or photocopying machine (to avoid using the local photocopying supplier, who could identify her after the fact), and she would have needed to arrange for some form of distribution other than passing out handbills at a public meeting. Compare McIntyre, 115 S Ct at 1522 (noting that the case "demonstrates [that] the absence of the author's name on a document does not necessarily protect either that person or a distributor of a forbidden document from being held responsible for compliance with the election code").
Thanks in large part to the easy availability of powerful cryptographic tools, the Internet provides the ability to send anonymous electronic messages at will. . . . [A]nonymously remailed email cannot, if properly implemented, be traced to its sender. In addition, two or more persons can communicate without knowing each other's identity, while preserving the "untraceable" nature of their communications.  

In cyberspace, a law prohibiting anonymous literature is not only of questionable constitutionality; it verges on incoherence. If Ohio, or any other jurisdiction, seriously wants to prohibit such communications, something other than a law declaring it illegal to communicate anonymously will be required, for in cyberspace we can no longer overlook the fact that perfect anonymity fatally challenges the enforceability of any laws prohibiting perfect anonymity.  

In a sense, there can be no more significant question regarding the structure of a legal system than that regarding the control of anonymous speech and anonymous conduct, for true anonymity goes to the heart of any attempt to impose the rule of law on any set of activities. But there is no well-developed and self-contained "jurisprudence of anonymity" in the nonvirtual world, because the scope for anonymous action is relatively limited; it would be hard to argue, for example, that the Supreme Court's  

---

21 Froomkin, Flood Control at 7 (cited in note 4) (emphasis added). Froomkin provides an excellent primer on the ways in which a combination of strong cryptography and the existence of "anonymous remailers"—mail services that "delete all the identifying information about incoming e-mails, [and] substitute a predefined header identifying the remailer as the sender or using a cute tag such as nobody@nowhere"—enable users to achieve virtually unbreakable anonymity. Id at 8-15. See also note 6.  

22 This is not to say that the availability of anonymous communication in cyberspace cannot be regulated in any fashion. The decentralized architecture of cyberspace and the difficulties of applying physically based notions of personal jurisdiction in an environment in which physical boundaries are difficult, if not impossible, to identify, may make direct enforcement of legal norms against individual violators more difficult once the means to accomplish such violation is widely disseminated. But as Perritt has noted, this decentralization "naturally shift[s] victim attention to intermediaries who are more likely to be readily identifiable, subject to the jurisdiction of traditional legal institutions, and financially able to pay compensation for injury." Henry H. Perritt, Jr., Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction (Paper presented at the University of Oslo, Oct 12, 1995) (unpublished manuscript on file with the University of Chicago Legal Forum). See also Niva Elkin-Koren, Copyright Law and Social Dialogue on the Information Superhighway: the Case Against Copyright Liability of Bulletin Board Operators, 13 Cardozo Arts & Enter L J 345, 399-411 (1995), for a particularly enlightening discussion of the relationship between decentralized systems and intermediary liability.
reasoning in *McIntyre v Ohio Elections Commission* is in any way central to an understanding of the American legal system. But in cyberspace, one can hardly imagine a legal question—from copyright infringement to the design of electronic banking and currency systems, from the regulation of obscene or indecent speech to the enforcement of libel law—that is not affected by questions regarding the scope and availability of anonymous communications.

If we are going to create a jurisprudence capable of reflecting intelligently on the new questions posed by the phenomenon of true anonymity, we will need to draw on learning from an expansive array of what previously have been scattered subdisciplines. Privacy law and the law of free expression come immediately to mind, and undoubtedly will have a significant role to play in this formulation. My suggestion here is simply that principles of great value for these purposes exist in another corner of the law that might not seem so obviously relevant, namely, corporation law. In order to see why this may be the case, however, a definitional detour is required to focus more clearly on the precise nature of the phenomenon in question here.

II. A DEFINITIONAL FRAMEWORK

Discussion of these questions requires, first, that we more carefully delineate the distinctions among three related concepts: anonymity, pseudonymity, and traceability. We begin with the notion that from the contents of a message the recipient may obtain information—a reduction in uncertainty—concerning

---


24 This framework expands upon the one first proposed by Froomkin. See A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases* 7-12 (Paper presented September 21, 1995 at the Conference for the Second Century of the University of Pittsburgh School of Law) (unpublished manuscript on file with the University of Chicago Legal Forum) (available online at http://www.law.miami.edu) (cited in note 4).

25 “Information” is used here in the information-theoretical sense, in which it is de-
the identity of the originator of the message. An “anonymous message” can be defined as a message that provides the recipient with no information—no reduction in uncertainty postreceipt when measured against the prereceipt baseline—concerning the identity of the message originator. This is a relatively straightforward and presumably noncontroversial definition; if I am no less uncertain about the identity of the message originator after I receive the message than I was before, the message is an anonymous one.

The degree to which a message can be considered anonymous cannot, however, always be determined solely with reference to the text of the message; it may require access to extratextual information about message context. Imagine, for example, that each of one hundred people receives the identical letter identified only as having been sent by “your friend.” Have they received an anonymous message? Some recipients certainly have—those who look at the identifying information and can extract nothing useful from it. For others, that particular string of characters may be quite meaningful; they may know some individual who frequently communicates with them in this precise way, and the message is therefore to them not anonymous at all.


Applied to the question at hand, an anonymous message is one in which the uncertainty (regarding the identity of the sender of the message) before the message is received is equal to the uncertainty after the message is received; in that case, we can say that the message contains no information about identity inasmuch as there has been no reduction in uncertainty achieved by receipt of the message. See, generally, Claude E. Shannon and Warren Weaver, *The Mathematical Theory of Communication* 18-26 (The University of Illinois Press, 1949); Marud Mansuripur, *Introduction to Information Theory* 1-4, 11-22 (Prentice-Hall, 1987).

A qualification of this definition might be helpful. One can certainly imagine truly anonymous messages in this strict sense: messages containing no information whatsoever about the originator of the message. However, it is probably more constructive to think of anonymity as a continuous, rather than a binary, attribute of messages; after all, even messages we ordinarily think of as “anonymous” contain some information about the author. For example, graffiti scrawled on a subway platform informs us that the author was literate and was physically present on that particular platform at some point during the period since the platform was last painted, all of which significantly reduces our uncertainty about the author's identity by ruling out the vast majority of individuals in the world as possible authors. In order to talk constructively about anonymous messages, we can think of there being some threshold of uncertainty-reduction, and define an anonymous message as one in which the amount of information regarding the originator of the message falls below this threshold.

26 More precisely, to those recipients the string of characters “your friend” conveys no uncertainty-reducing information at all. See note 25.
Moreover, the amount of identifying information contained in a message is rarely a fixed quantity; relevant information may often be available, but only at some additional cost or effort. This letter from "your friend" may be anonymous when I receive it, but there may be ways that I can obtain additional information that narrows down the list of potential originators. It may, for example, be covered with fingerprints from which, were I able easily to access both a fingerprint reader and a comprehensive database of fingerprints, I could obtain significant information about likely originators.

We can define a second variable—"traceability"—to measure the ease with which additional information of this kind about the identity of the sender can be obtained. Traceability, like anonymity, is highly context-dependent; the cost of obtaining a given amount of additional identification information will vary, possibly greatly, from one situation to another. In the example above, the traceability of the message is technology-dependent; that is, traceability will vary depending on whether the fingerprint reader and database are available to the recipient. More commonly, relevant identification information may exist in the hands of third parties (parties other than the originator and recipient). If instead of a letter I receive an anonymous e-mail bearing the return address "yourfriend@someplace.org," I may be able to obtain information about the location of the "someplace.org" domain and the identity of the owner,28 who may be able to reveal the name and address of the individual to whom the "yourfriend" ID was assigned. In the case of e-mail arriving from an anony-

---

mous remailer, the owner of the remailer may retain the identification information that was present in the incoming message. Where this is the case, the traceability of a message may be largely a function of the remailer’s duty (or lack of a duty) to keep the information secret and the ease with which disclosure can be legally compelled (by process, subpoena, warrant, or otherwise). It may be relatively easy for a law enforcement official to obtain the name and address of the individual who has been assigned the “yourfriend” ID, while the same information may be extremely difficult and costly for other individuals (including the recipient) to obtain.

One final complication will complete this definitional framework: pseudonymity. Assume for the moment a context in which these letters (or e-mail messages) are untraceably anonymous, as defined above. Assume further that you receive a series of such letters or e-mails, all bearing the same signature (electronic or otherwise). Over time, it becomes less and less constructive to think of these messages as merely anonymous, even though you may come no closer to identifying the actual, biological individuals responsible for them. As you come to associate certain characteristics with the fictional entity associated with the identifier “your friend”—grammar, spelling, style, forcefulness of rhetoric, reasonableness of argument, and so on—it becomes increasingly useful to recognize that “your friend,” whoever or whatever it may be, is the message originator. “Your friend,” in short, has become a pseudonym.

29 This phenomenon was most clearly illustrated in February 1995, when officials of the Church of Scientology engaged in a series of disputes with individuals who had been using the anon.penet.fi anonymous remailer to post documents to the alt.religion.scientology Usenet group. According to the Church, these documents contained copyrighted and trade-secret information. The Church enlisted the aid of the Finnish police and obtained a warrant for a search of the anon.penet.fi database. See A. Michael Froomkin, Anonymity and Its Enmities, 1995 J Online L art 4, ¶ 40 (http://www.law.cornell.edu/jol/jol.table.html) (cited in note 6); David Post, The First Internet War: Scientology, its Critics, Anarchy, and Law in Cyberspace, Reason 28 (Apr 1996). Information on this incident is also available at http://www.cybercom.net/-rnewman/scientology/home.html#PENET.

30 As a general matter, information about the identity of the author(s) of an e-mail message does not appear to be protected under U.S. law. While the Electronic Communications Privacy Act, 18 USC §§ 2510 et seq (1994), prohibits (with certain exceptions) the disclosure of “the contents of any . . . electronic communication,” 18 USC §§ 2511(c), 2511(e)(i), the statute does not similarly protect the name or address of the originator of the message. Accordingly, it does not appear that third party system operators or administrators have a statutory duty to disclose, or to refrain from disclosing, such information.
The above simple example makes clear that the distinction between anonymous and pseudonymous messages is a subtle one. The first time that a novel was published under the name “Mark Twain,” one appropriately may have considered this an “anonymous” text, the equivalent of publication under the name “Anon.” I obtain no more information about the identity of the “true”—biological—author of the book in the former case than in the latter. Why then is “Mark Twain” considered a pseudonym while “Anon.” is not? The answer, of course, is that just as with “your friend,” over time the identifier “Mark Twain” came to be associated with a distinct set of characteristics that may be considered assets—“reputational capital”—of the pseudonym itself. Without these associations there is indeed no meaningful difference between anonymity and pseudonymity; had Samuel Clemens chosen to publish each of his novels under a different pseudonym, that would have been essentially equivalent to publishing all of his novels under the single pseudonym “Anon.” or “John Doe.” But by the time The Adventures of Huckleberry Finn was published, we could no longer say that the designation of “Mark Twain” as the author gave us no information about the originator of the text; the originator of the text is the fictional entity Mark Twain.

Let me propose the following working definition: a “pseudonymous message” is (a) a message that is anonymous (in the sense that it provides no information concerning the identity of the biological individual or individuals responsible for preparing or transmitting the message), but that (b) contains some information about the identity of some cognizable entity that is the originator of the message.

III. ANONYMITY AND PSEUDONYMITY IN CYBERSPACE

What light can this framework shed on the question of whether, or how best, to regulate the availability and use of anonymous messaging in cyberspace? In order to focus this discussion in a concrete way, let me start by setting up something of a straw man: assume that the Ohio legislature were to attempt to ban anonymity in cyberspace by passing a statute with a disclosure provision identical to the one at issue in McIntyre v Ohio Elections Commission, 31 but applicable only to electronic communications. This law would require that all computer-medi-

---

ated electronic communications disclose the "name and residence or business address of the chairman, treasurer, or secretary of the organization issuing" the communication, or the name and residence of the "person who issues, makes, or is responsible" for it.\(^{32}\)

An assumption may help to focus attention on some of the less obvious consequences of this disclosure requirement. In *McIntyre*, Justice Ginsburg left open the possibility that the disclosure requirement struck down in that specific context might be constitutionally permissible elsewhere:

The Court's decision finds unnecessary, overintrusive, and inconsistent with American ideals the State's imposition of a fine on an individual leafleteer who, within her local community, spoke her mind, but sometimes not her name. We do not thereby hold that the State may not in other, larger circumstances, require the speaker to disclose its interest by disclosing its identity.\(^{33}\)

Assume that cyberspace is one of those "larger circumstances." That is, assume that the harms flowing from the easy availability of truly anonymous messaging in cyberspace—the ability to freely discuss terrorist tactics, or the comparative effectiveness of bomb-making formulas, etc., on the Internet without fear of any law enforcement interference—have so substantially increased that they are precisely equal to the benefits flowing from such speech.

This assumption is unlikely to be correct. It enables us, however, to disaggregate the effects of this hypothetical statute on truly anonymous speech from its effects on pseudonymous speech by imagining a context in which the cost-benefit balance is in equipoise in regard to truly anonymous communication, and then asking: what other costs and benefits might be associated with this statutory disclosure provision?\(^{34}\)

---

\(^{32}\) The scope of Ohio's jurisdiction to impose this hypothetical statutory scheme is an important and complex question. See Henry H. Perritt, *Jurisdiction in Cyberspace* (Paper presented at Villanova Law Review Symposium, Oct 28, 1995) (unpublished draft on file with the University of Chicago Legal Forum). Also important is the question of how any such rule would be enforced against violators in cyberspace. Any comprehensive attempt to analyze the consequences of this statute would need to address these questions, but I will not do so here, in order to focus attention on a different set of issues.

\(^{33}\) *McIntyre*, 115 S Ct at 1524 (Ginsburg concurring).

\(^{34}\) Note that I am not asking precisely the same question the Court in *McIntyre* asked with reference to the real-world equivalent of this statute, namely, whether it complies with the First Amendment of the U.S. Constitution. See *McIntyre*, 115 S Ct at 1514.
Note first that, at least under my definitions, pseudonymity is a subset of anonymity: a pseudonymous message is an anonymous message, containing no information about the "actual" identity of the message originator (although a pseudonymous message does contain certain other identifying information). That being the case, eliminating the entire category of anonymous messages—"banning anonymity"—effectively eliminates all pseudonymous messages as well.

Even regulations falling short of a total ban on anonymous messaging are likely to eliminate pseudonymity to the same extent they eliminate anonymity. The reason is that it is difficult to distinguish between these two subsets of anonymous messages—what I call "truly anonymous" (that is, nonpseudonymous) and pseudonymous messages—because the distinction between them is, as noted above, necessarily context-dependent. Characterization of a message as falling within one or the other of these categories can rarely be accomplished solely with reference to the message text itself. As in the examples above, we may only be able to determine whether an electronic-mail message from "your friend" or "Mark Twain" is pseudonymous from the historical context in which the message is embedded, the process by which strings of characters have, or have not, become associated with particular identifying characteristics. It is unlikely that sufficient information about context can be captured by any rule that attempts to regulate the transmission of anonymous messages; this contextual information is likely to be invisible to anyone monitoring message content. Therefore, any such rule will be unlikely to distinguish between truly anonymous and pseudonymous messages, and correspondingly likely to sweep all forms of pseudonymity into its enforcement web as well.

The McIntyre Court implicitly recognized this principle that restrictions on anonymity necessarily restrict pseudonymity as well. The Court made frequent reference to the Federalist Papers and other pseudonymously published material in support

---

Whether this hypothetical statute is constitutional as applied to electronic communications is of course an important question. But for reasons examined in detail elsewhere, see David R. Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace, (forthcoming Stan L Rev) (1996) (unpublished manuscript on file with the University of Chicago Legal Forum) (cited in note 2), and reasonably well summarized by the aphorism that "the First Amendment is a local ordinance in cyberspace," I prefer, in the global context of cyberspace, to direct my attention to the underlying policy question of the wisdom of such a scheme rather than its compliance with any particular set of "local" standards.

35 McIntyre, 115 S Ct at 1517 n 6.
of its analysis of the benefits that society derives from anonymous communication.\textsuperscript{36} The Court observed that the "respected tradition of anonymity in the advocacy of political causes" is "most famously embodied in the Federalist Papers, authored by James Madison, Alexander Hamilton, and John Jay, but signed 'Publius,'"\textsuperscript{37} and Justice Thomas noted that the Federalist Papers are "only the most famous example of the outpouring of anonymous political writing that occurred during the ratification of the Constitution."\textsuperscript{38} I have no doubt that the Justices of the Supreme Court are capable of distinguishing between anonymous and pseudonymous communication should the need arise; but in regard to this statute the need did not arise precisely because the statute had identical effects on both forms of communication. Anyone found distributing the pseudonymously published Federalist Papers in Ohio (including, but not limited to, Messrs. Madison, Hamilton, or Jay) would have suffered the same fate as Mrs. McIntyre. As a result, the Court correctly took into account the costs of suppressing socially valuable pseudonymous works when evaluating Ohio's prohibition on anonymous communication, and concluded, in effect, that the aggregate social costs of eliminating both forms of speech were not outweighed by the State's asserted interests.\textsuperscript{39}

\textsuperscript{36} The Federalist Papers, of course, are within the subset of anonymous works that can be considered pseudonymously published; the "true identity" of the authors is not revealed in the communications themselves, but the entity responsible for authorship—"Publius"—is conspicuously communicated. See, for example, Federalist 9 (Hamilton), in Clinton Rossiter, ed, The Federalist Papers 71, 76 (Mentor, 1961).
\textsuperscript{37} McIntyre, 115 S Ct at 1517 n 6.
\textsuperscript{38} Id at 1526 (Thomas concurring). The majority observed that:

Publius's opponents, the Anti-Federalists, also tended to publish under pseudonyms: prominent among them were "Cato," believed to be New York Governor George Clinton; "Centinel," probably Samuel Bryan or his father, Pennsylvania judge and legislator George Bryan; "The Federal Farmer," who may have been Richard Henry Lee, a Virginia member of the Continental Congress and a signer of the Declaration of Independence; and "Brutus," who may have been Robert Yates, a New York Supreme Court justice who walked out on the Constitutional Convention. A forerunner of all of these writers was the pre-Revolutionary War English pamphleteer "Junius," whose true identity remains a mystery.

Id at 1517 n 6 (citations omitted). See also Talley v California, 362 US 61, 65 (1960) ("Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.").
\textsuperscript{39} McIntyre, 115 S Ct at 1520-22 (discussing the two state interests proffered by Ohio in support of this statutory provision: the "interest in providing the electorate with relevant information" and in "preventing fraudulent and libelous statements").
Is it so obvious that the Ohio statute would have banned distribution of the *Federalist Papers*? Recall the relevant statutory language:

No person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to . . . promote the adoption or defeat of any issue, . . . through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefor.\(^4\)

Clearly, the *Federalist Papers* do not comply with the statutory disclosure requirements: no “name and residence or business address” is set forth in that publication. But notice that the pseudonymous author (“Publius”) could not have complied with this disclosure requirement. Even if “Publius” were a “person” within the meaning of the statute, it had no “residence or business address,” and if it were deemed not a “person” but an “organization issuing the communication,” it had (as far as we know) no “chairman, treasurer, or secretary” whose name could be disclosed.

“Publius,” in other words, was not the kind of entity permitted by the Ohio authorities to engage in this form of public discourse, for the Ohio statute explicitly required that communications come exclusively either from “persons,” or from “organizations” that have a particular structure (namely, that have an identifiable “chairman, treasurer, or secretary”).\(^4\) By calling for the disclosure of certain information, the statute implicitly required that the information exist; if the information did not exist, the statutory requirements could not be complied with. Although the statute ostensibly regulated only the disclosure of certain information, it was in fact regulating the kinds of entities that


\[^4\] The statute also permitted publications “issued by the regularly constituted central or executive committee of a political party, organized as provided in Chapter 3517 of the [Ohio] Revised code,” provided that they bore “the name of the committee and its chairman or treasurer.” *Id.*
would be allowed to participate in the public debate. Any association of individuals—the "Concerned Parents and Taxpayers," or the shareholders of "McDonalds, Inc.," or the members of the Class of 1998 of Blendon Middle School or of the faculty of the Georgetown University Law Center—was more than welcome to participate, provided that it first organized itself in such a fashion that it have a "chairman, treasurer or secretary." Only then, after the relevant information was created, could the second statutory requirement—that the information in those categories be disclosed—be applied.

Viewed in this light—as a requirement that certain organizational formalities be complied with before action under an organizational pseudonym can be taken—the Ohio statute more closely resembles a species of "corporate law." It is a regulation of the way that individuals may combine their collective efforts into organizational forms and take action of various kinds. This may seem a rather strained reading of this statute, and it is certainly not the reading that the Court gave to it. But the Court's reading may simply reflect the fact that the Ohio authorities chose to prosecute Mrs. McIntyre, the individual caught distributing the offending leaflets, rather than "Concerned Parents and Taxpayers," the "organization" ostensibly responsible for preparing them.

On reflection, we should not be surprised by the close link between questions regarding regulation of pseudonymous communication and corporate law (or any other means of regulating "legal personhood"). Pseudonymity, after all, is the process by which nonhuman entities acquire names under which they can take action, and the body of corporate law is one way that the legal system controls the recognition of such entities:

[P]hysical human beings are not the only entities protected at law, nor the only entities that have rights.

42 Had Ohio proceeded against this collective entity (that we may assume had neither a business address nor a "chairman, treasurer or secretary" within the meaning of the statute), could the organizational defendant have argued that the statute unconstitutionally abridged its freedom of speech by shutting out certain entities from participation in the public debate? In such a posture, the case would more closely have resembled First National Bank of Boston v Bellotti, 435 US 765 (1978), in which the Court more directly confronted the constitutionality of prohibiting certain legally recognized entities from participating in communicative activities when it struck down a Massachusetts statute prohibiting any corporation from expending funds "for the purpose of... influencing or affecting the vote on any question submitted to the voters, other than one materially affecting any of the property, business, or assets of the corporation." Id at 768.
And routine doctrines of standing (the analysis of who—or what—may bring a lawsuit or complain about an asserted violation of rights) have traditionally comprehended more than individual, physical, human beings.

Most obviously, corporations, partnerships, and associations have substantive rights, and have the procedural right to bring suit. They also have rights to due process of law, to have those substantive rights enforced. Companies sue, and can be sued; they have lawyers and can invoke first amendment rights to free speech. All of this is quite separate, by definition and intent, from the rights and liabilities of the individual human beings who jointly own the company.

The law abounds in further examples: we find a plethora of specific entities with rights and standing to sue or be sued, and quasi-entities, or procedures which dispense with the need for the specific real humans who have the real interest in the lawsuit.43

We are surrounded by pseudonymous communication issued by fictional beings every day. For example, though we do not generally think of corporate speech as an example of pseudonymous speech, it clearly falls within that category. When I receive an advertising flyer from my local McDonald's restaurant, identified only by a prominently placed corporate logo (the familiar “golden arches”), the message is an “anonymous” one, inasmuch as it contains no information at all about the identity of the individual(s) who may have typed it up, reproduced it, or placed it under my door. But it is also clearly within the subset of pseudonymous messages because the presence of the logo provides a great deal of information about the recognizable (corporate) entity responsible for preparing and distributing the flyer.44

The syllogism, then, is as follows: the regulation of anonymous communication is inextricably linked to the regulation of pseudonymous communication; the latter is, in turn, inextricably


44 That information may, or may not, be reliable or trustworthy; a competitor may have forged the McDonald's logo, for example. The reliability of this information is, at least to some extent, a function of the legal protection afforded to this form of information through, for example, trademark law.
linked to the regulation of the varieties of "legal persons" that the law will recognize, the kinds of collective entities that will (or will not) be permitted to engage in public discourse or other activities; therefore, the regulation of anonymity is inextricably linked to the determination of which entities the law will recognize and allow to participate in public discourse or other activities. In fact, the relationship between pseudonymity and these latter questions can profitably be extended still further. We are well acquainted with the notion that some collective entities ("corporations") to which the law grants fictional legal personhood are formed by the operation of statutory provisions that limit the liability of the individuals participating in those entities (shareholders) for the entity's actions. These provisions allow those individuals to contribute tangible assets to the collective entity while remaining (relatively) secure in the knowledge that only those contributions, and not any other of the individuals' assets, are at risk when the collective entity acts.45

Pseudonymity itself is a means, independent of these statutory provisions, for achieving much the same limited-liability goal for participants in collective-communicative activities. By definition, a pseudonymous communication contains no information about the identity of the individual(s) truly responsible for the communication. To the extent—but only to the extent—the communication is untraceably pseudonymous, damage to or depletion of the tangible assets belonging to the actual speaker(s) may be avoided by virtue of the fact that (by definition) there is no feasible way to identify those speakers. If I am unable to determine the true identity of the individual or individuals constituting "your friend" or "Mark Twain" or "Concerned Parents and Taxpayers" (or the shareholders of "McDonalds, Inc."), I can look no further than

45 Limited liability, a fundamental principle of corporate law, requires that shareholders in a corporation are not liable for the obligations of the enterprise beyond the capital that they contribute in exchange for their shares. See Model Business Corp Act § 6.22(b) (Harcourt Brace Jovanovich, 1985). Limited liability was not always the rule in American law. See Stephen B. Presser, Thwarting the Killing of the Corporation: Limited Liability, Democracy, and Economics, 87 Nw U L Rev 148, 155-56 (1992) (discussing the historical background of adoption of limited liability statutes); Phillip I. Blumberg, Limited Liability and Corporate Groups, 11 J Corp L 573, 587-95 (1986) (describing early American law providing for shareholder liability). However, it has been accepted in most American jurisdictions since the mid-nineteenth century. Blumberg, 11 J Corp L at 591-95 (limited liability was the rule by the middle of the nineteenth century with several exceptions that continued into the twentieth century). See also Robert B. Thompson, Piercing the Corporate Veil: an Empirical Study, 76 Cornell L Rev 1036, 1039 (1991).
the assets of the entity itself, if any, (or, perhaps, to some third party) for compensation.

This form of limited liability is also a characteristic, to be sure, of anonymous speech; indeed it is but a restatement of the rather obvious point that truly anonymous speakers may avoid being held accountable for any harms arising from their speech. But pseudonymity brings potentially offsetting benefits into play: by serving as storehouses of reputational capital, pseudonymous entities add value to social interaction in a way that anonymous speech does not. It is on the nature of that additional value, I suggest, that we need to focus our attention if we are to intelligently regulate anonymity in cyberspace. In the corporate context, society adopted limited liability as a conscious strategy to encourage the pooling of physical and financial assets and to induce individuals to take socially useful collective action. In cyberspace, the same considerations should inform the extent to which we protect pseudonymous communication. That is, any regulation should be informed by the social benefits that these pseudonymous entities produce and the extent to which this form of limited liability is required to induce “investors” (participants in these pseudonymous entities) to pool their intellectual capital into such entities.

Even given my initial assumption—conceding a heightened potential for harm from truly anonymous speech in the special circumstances of cyberspace—our understanding of the overall balance between costs and benefits of a ban on anonymity is not complete until we examine the effect that this ban may have on the formation of collective pseudonymously speaking entities. A simple ban on anonymity (such as the one the hypothetical Ohio legislature has tried to impose) denies us the benefits that may be gained from the activities of entities of this kind; a more nuanced approach may enable us to capture at least some of those

---

46 See Richard A. Posner, Privacy, Secrecy, and Reputation, 28 Buff L Rev 1, 31 (1979) ("Reputation has an important economic function in a market system (or in any system where voluntary interactions are important). It reduces the search costs of buyers and sellers, makes it easier for the superior producer to increase his sales relative to those of inferior ones, and in these ways helps channel resources into their most valuable employments—a process at the heart of the market system. This role is not limited to explicit markets; it is just as vital to the functioning of the 'marriage market,' the market in friends, the political market, and so on."). See also Elmer William Hanak, III, The Quality Assurance Function of Trademarks, 43 Fordham L Rev 363, 364 (1974); William M. Landes and Richard A. Posner, Trademark Law: An Economic Perspective, 30 J L & Econ 265 (1987).

47 See notes 8-11 and accompanying text.
benefits while simultaneously minimizing the harms attendant on an anonymous messaging system. Corporation law has a long history of attempting to strike that balance, and I propose that we begin developing a form of corporate law for cyberspace, rules regarding the formation of these entities and the protections that they will be afforded, in order to competently address the (seemingly unrelated) question of the regulation of anonymous speech. We need, in other words, to ask a series of questions about our hypothetical ban on anonymity that have little (if anything) to do with the continued existence of anonymous remailers or the mechanics of chained encryption. Are the kinds of collective entities that can be formed in cyberspace sufficiently valuable that we should induce individuals to form them by offering limited liability? If so, how might our rules regarding traceability be fashioned to maximize those benefits? In what contexts should we allow, or require, any form of “piercing the pseudonymity veil” (and how might we ensure that the information required to perform that operation is available)?

Designing limited-liability/pseudonymity rules for cyberspace will probably be no easier than designing them for the nonvirtual world, where there is something of a “consensus that the whole area of limited liability, and conversely of piercing the corporate veil, is among the most confusing in corporate law.” Many commentators have suggested abandoning limited liability in the corporate context altogether; others have come to its defense on assorted grounds. I will content myself with the following observations regarding what I believe to be some of the features that this analysis will require.

First, it seems plausible to assert that the unique characteristics of cyberspace so enhance individuals’ ability to pool their

---


49 These arguments are summarized in Thompson, 76 Cornell L Rev at 1039-1043 (cited in note 45).
intellectual capital into entities of this kind that the benefits to be gained by allowing and encouraging these forms of intellectual undertakings are likely to be substantial. One of the ways in which cyberspace differs from the nonvirtual world is precisely the remarkable and astonishing ease with which collective entities of various kinds—some of which look like little that we have previously encountered—can be formed; there are, at present, no registration requirements, no forms that need to be filled out, no approval that needs to be obtained, in order to call these entities into existence. The fundamental characteristic of cyberspace is that it is a network (or, more properly, a network of networks); everyone in cyberspace is connected to everyone else through the magic of interconnectivity protocols\(^5^0\) and can communicate instantaneously on a one-to-one, one-to-many, many-to-one, or many-to-many basis with a constantly shifting (but enormous) population of other individuals. In the space of an afternoon, I can join a dozen (or a hundred) ongoing associations by subscribing to individual listservers or Usenet discussion groups, form a dozen new such associations myself with a few lines of code inserted in my Internet Service Provider’s system, and set up a dozen aliases on my provider’s mail system through which I can communicate (and invite friends and colleagues to help me formulate the messages that will go out under each of these aliases).\(^5^1\) Fictitious entities of this kind, speaking through pseud-


\(^5^1\) See Eugene Volokh, Cheap Speech and What It Will Do, 104 Yale L J 1805, 1833-43 (1995). I have described this phenomenon of low-cost association building in the context of the ongoing battles in cyberspace between the Church of Scientology and some of its critics over alleged unlawful postings of copyrighted and trade secret material:

[Relations between [Scientology's] adherents and critics have never been pleasant; passions run feverishly high on both sides, and the Scientologists have often been accused of dealing, shall we say, rather harshly with their critics.

But at least until July 17, 1991, there was no truly organized opposition to the Scientologists's teachings and tactics, no true community of the disaffected. How could there be? Building an anti-church, after all, takes just about as much administrative and operational savvy, not to mention money, as does building a church. But that feature of the landscape changed dramatically on the date mentioned, when a Scientology critic, Scott Goehring, formed a discussion
onyms, are ubiquitous in cyberspace, a remarkable feature of the new landscape that is sometimes taken for granted.\textsuperscript{52} Two (or more) heads are—surely in some circumstances at least—better than one. The prospect for more creative uses of this ability for individuals to pool their intellectual capital with great flexibility and with a minimum of start-up or transaction costs into a wide range of new kinds of actors and entities—what Howard Rheingold has called "grassroots groupmind"\textsuperscript{53}—each capable of establishing a unique identity and accumulating its own specific reputational capital, is a profound and exciting feature of cyberspace.\textsuperscript{54}

———

group—"alt.religion.scientology"—on what is called the "Usenet" network portion of the Internet. . . . Suddenly, in the 30 seconds or so that it took Goehring to type out his request, and the $0.05 or so it cost him to transmit that message to the computers responsible for Usenet network configuration, there is a place where the disgruntled can meet to exchange ideas and information—a new community, one of the literally hundreds of thousands of such communities that have sprung into being on the Internet over the past few years.

David Post, The First Internet War: Scientology, Its Critics, Anarchy, and Law in Cyberspace, Reason 28 (Apr 1996) (cited in note 29). We may often describe a Usenet group such as alt.religion.scientology as a "place," as I have in the above excerpt; but it may also properly be considered a "person" or an "association" consisting of its members at any given time.

\textsuperscript{52} The use of "screen names" on commercial online services is virtually universal, and though we often assume that there is one individual standing behind each such name, that assumption is usually just that—an assumption—without any particular foundation. For example, as noted above, the ideas in this paper were developed during a number of online discussions with "Perry the Cynic," [perry@cynic.org]; I have not been able to confirm that this is, or is not, a single individual.

\textsuperscript{53} Howard Rheingold, The Virtual Community ch 4 (Addison-Wesley, 1993) ("[G]roups of people are using [computer-mediated communication] to rediscover the power of cooperation, turning cooperation into a game, a way of life—a merger of knowledge capital, social capital, and communion. The fact that we need computer networks to recapture the sense of cooperative spirit that so many people seemed to lose when we gained all this technology is a painful irony.").

\textsuperscript{54} My favorite example of this phenomenon is the Cancelmoose, a fictitious being operating pseudonymously in cyberspace that has taken a lead in issuing "cancelbots"—commands that cancel postings to Usenet newsgroups—in response to reported instances of "spamming" (bombarding numerous newsgroups with copies of the same message). One answer to the question "Who is Cancelmoose[tm]?” is provided in the Frequently Asked Question ("FAQ") file for the Usenet newsgroup news.admin.net-abuse (Nov 15, 1995 version) (available online at http://www.smartpages.com/faqs/net-abuse-faq/part1/faq.html and http://www.smartpages.com/faqs/net-abuse/faq/part2/faq.html).

Cancelmoose[tm] is, to misquote some wise poster, "the greatest public servant the net has seen in quite some time." Once upon a time, the moose would send out spam-cancels and then post notices anonymously to news.admin.policy, news.admin.misc, and a.c.e.n.a. The Moose stepped to the fore on its own initiative, at a time (mid 1994) when spam-cancels were irregular and disorganized, and behaved altogether admirably—fair, even-handed, and quick to respond to comments and criticism, all without self-aggrandizement or martyrdom.
There is a "democratizing" impulse at work here, a relatively sudden increase in each individual cyberspace citizen's ability to participate in public collective action without formalities or legal barriers of any kind. Just as the doctrine of corporate limited liability itself developed as a means of encouraging individual entrepreneurial participation in the economic life of the nation, so too should the benefits of these new forms of public participation be weighed carefully before adopting any regulation of anonymity. The question is not whether there are costs associated with the activities of these entities (for surely there are), nor whether those costs could be lowered by imposing a stringent traceability regime denying all participants in these entities the liability shield of pseudonymity (for that, too, is clear). The ques-

---

Cancelmoose\[tm\] quickly gained near-unanimous support from the readership of all three above-mentioned groups. Nobody knows who Cancelmoose[tm] really is, and there aren't really any good rumors. However, the moose now has an e-mail address (moose@cm.org) and a web site (http://www.cm.org.).

See Benjamin Wittes, Law in Cyberspace: Witnessing the Birth of a Legal System on the Net, Legal Times S27-29 (Jan 23, 1995) (describing Cancelmoose as "widely seen not as a censor but as an enforcer of the accepted rules of Usenet.

Cancelmoose is a fascinating example of the Net's self-government because of the care he takes to avoid going beyond the community's consensus on which cancels are legitimate. He posts a justification for each of his cancels on a newsgroup devoted to net abuse, including in that justification a copy of the original message and a list of the newsgroups from which the spam was removed. He also includes information allowing sysops to override the cancels. Cancelmoose also takes pains to emphasize that the content of messages does not influence his decision whether or not to cancel them.

Kevin M. Savetz, Terminators: Net Guardians are Launching Cancelbots to Devour Unpalatable Spam, Internet World 80 (June 1995). Cancelmoose has also been described as an "Internet terrorist," "the first lawman of the electronic frontier," see Katz, Snapshots: Moose on Loose, The Guardian 8 (Dec 22, 1994), and, interestingly, as "a hacker's program," see Todd Copilevitz, Imposter Using Internet to Make Author's Life Miserable, Dallas Morning News 5A (Dec 21, 1994).

Whether the Cancelmoose is a single person, a collective entity acting under the name of Cancelmoose, or lines of code—a "hacker's program" designed to take action against particular kinds of spamming incidents—is, as far as I am aware, not known and may well be unknowable given today's technology (and the absence of Net-wide rules governing the obligation to disclose personal identity). Whatever it may be, it has, of course, its own home page. See http://www.cm.org.

55 See Presser, 87 Nw U L Rev at 155-156 (cited in note 45); Stephen B. Presser, Piercing the Corporate Veil § 1.03 at 1-14 (Clark Boardman Callaghan, 1993); Paul Halpern, Michael Trebikock, and Stuart Turnbull, An Economic Analysis of Limited Liability in Corporation Law, 30 U Toronto L J 117, 118-19 (1980) (discussing the arguments in support of limited liability in England regarding its expected effects on the "investments of savings by the middle and working classes").

tion is, rather, whether we may need to bear those costs in order to reap the benefits from these "groupmind" activities. I have no answer to this question, but such considerations surely should give us pause when confronted with any effort to eliminate anonymity—and, by extension, pseudonymity—in cyberspace.

Second, we should be particularly solicitous of mechanisms in cyberspace that, like pseudonymous speech, can serve as vehicles for investment in reputational capital. Cyberspace resembles a "state of nature" in many respects, notably in the absence of effective centralized mechanisms for the enforcement of legal rules. As Rubin has persuasively argued, in such an environment institutions that allow "firms" (that is, collective entities of various kinds) to accumulate and protect reputational capital are of paramount importance. The notion of the "state of nature," of course, dates back at least to Hobbes. See Thomas Hobbes, *Leviathan* 100, 108 (Macmillan Publishing Co., 1962) (originally published in 1651) ("[D]uring the time men live without a common power to keep them all in awe, they are in that condition which is called war; and such a war, as is of every man, against every man. ... If a covenant be made, wherein neither of the parties perform presently, but trust one another; in the condition of mere nature. ... it is void: but if there be a common power set over them both, with right and force sufficient to compel performance, it is not void."). See also Anthony T. Kronman, *Contract Law and the State of Nature*, 1 J L Econ & Organization 5, 6-9 (1985) (defining the state of nature between two parties as the situation "[w]hen two individuals (or groups) exchange promises and neither has the power to compel the other to perform, and there is also no third party powerful enough to enforce the agreement on their behalf"). The global nature of the electronic networks constituting cyberspace and the absence of a "common power to keep [participants] in awe" make it plausible to suggest that cyberspace has many features that resemble the state of nature. See Post, *Reason* at 28 (cited in note 29).

Rubin writes:

[Private mechanisms for solving the problems associated with opportunism in transactions [are] limited in their power; they cannot achieve an optimum. Without efficient government enforcement, it will be impossible to realize all potential gains from trade. ... On the other hand, it is possible to underestimate the power of such [private] mechanisms. ... In a world where trade is legal but contracts are not enforced, ... reputations can become public knowledge, giving much more power to these [private] mechanisms. ... There are three classes of private mechanisms to make agreements credible. All three rely on reputations.

Note also that pseudonymity limits participants' liability in another way: speaking through an untraceable pseudonym shields the intangible personal assets of the speaker or speakers—their own private reputations and the constellation of personal characteristics associated with their true identities—from any damage resulting from the action of the pseudonymous entity. The storehouse of intangible reputational capital of that entity—"Publius," for example—may become depleted without any effect on Alexander Hamilton's reputation, and vice versa.

One characteristic of reputational capital and the privacy interests that may be affected by disclosure of individual identity is that the value of these interests for the individual is not easily transferable to third parties. For example, it may not be possible to use the reputational capital of the individual participants in a pseudonymous entity to compensate someone who was harmed by that entity's actions. If you have been harmed by the actions taken by, say, the pseudonymous entity Cancelmoose, disclosure that Cancelmoose is actually Johan Helsingius (the proprietor of a well-known anonymous remailer in Finland) and Mother Teresa, acting in concert, will not, standing alone, compensate you for that harm.

Disclosure may, however, damage the reputational capital that those two individuals can draw upon in their other efforts, and it may persuade others that the risk of participating in enterprises of this kind is not worth the possible cost to their own reputations or privacy interests, but those costs are not paid over to you as the aggrieved party. In some circumstances, of course, this information may be instrumental in obtaining compensation by allowing you to locate the responsible actors and to proceed against them as individuals. In other circumstances, however, this information will not lead to compensation, and the loss of value associated with the disclosure of this information is not matched by any corresponding gain to the aggrieved party.

Protecting the valuable "limited liability" features of pseudonymity need not, however, mean that harms imposed on third parties by pseudonymous entities must go unredressed. The

(cited in note 6). These suggestions closely parallel Rubin's call for such protection in the context of the newly emerging Eastern European democracies. Rubin, 27 Cornell Intl L J at 35-36 ("The most important assistance governments can give to private firms to create reputation capital is a willingness to enforce trademark property rights.").

59 If, for example, you are unable to obtain jurisdiction over the individual participants whose identities have been revealed, or there is no cause of action for the harm you have suffered under the laws of the jurisdiction in which they are located.
need to protect both third parties and the individuals that make up pseudonymous entities calls for an exploration of alternative traceability rules⁶⁰ that perhaps can be drawn carefully to maximize the likelihood of compensating victims of unlawful conduct—such as third party insurance or bonding requirements that allow redress to be achieved without exposing participants’ personal identities to risk⁶¹—while simultaneously minimizing the losses that may be attendant upon disclosure.

CONCLUSION

There have, up to now, been few steps to regulate anonymous speech in cyberspace—indeed, it is unclear how one would implement and enforce such regulation—but attempts to take such steps are surely on the horizon. The harms attendant on anonymous speech are often more easily recognized and more spectacular⁶² than the sometimes subtle benefits it may produce. Having begun this Article with reference to calls for the regulation of the availability of anonymous speech in cyberspace, I

---

⁶⁰ Because of the key role that rules regarding intermediary liability play and will play in cyberspace, see note 22, and the critical importance of traceability in determining whether pseudonymity plays an effective role in limiting liability, see notes 28-30, 36-37 and accompanying text, it is likely that whatever regulation is imposed in an attempt to control anonymous or pseudonymous communications will be imposed on network intermediaries through, for example, rules regarding their duty (a) to collect verifiable identifying information from subscribers, (b) to turn over that information in specified circumstances, and (c) to refuse to carry communications that come from systems that do not abide by similar traceability rules.

⁶¹ This is equivalent to a corporate law with a "minimum capitalization" requirement but without a corresponding absolute right to inspect shareholder lists. Nearly all states give shareholders some right to inspect corporate records, which may include the shareholder list, upon proper showing of need. See, for example, 8 Del Code Ann § 220(b) (1994) (providing that any stockholder shall have the right to "inspect for any proper purpose" the corporation's list of stockholders, and defining "proper purpose" as "a purpose reasonably related to such person's interests as a stockholder"); Model Bus Corp Act § 16.02(c) (Prentice Hall Law & Business, 1991) (allowing inspection of the shareholder list if the inspecting shareholder makes his demand "in good faith and for a proper purpose" and shows that the records are "directly connected with this purpose"); Cal Corp Code § 1600 (West Supp 1986) (providing that shareholders holding at least 5 percent in the aggregate of the outstanding voting shares of a corporation have "an absolute right" to inspect and copy the record of shareholders' names and addresses). See also SEC Rule 14a-7, 17 CFR § 240.14a-7(a) (1995), under which a shareholder, subject to some restraints, may require the corporation engaged in a proxy solicitation to choose either to provide a shareholder list to the shareholder or to mail the shareholder's soliciting materials, if any, to other shareholders (at the shareholder's expense).

⁶² The day surely will come when law enforcement authorities report that a serious crime was planned by means of anonymous electronic communication. It is equally certain that the popular press will react with horror, and that calls for a prohibition on this kind of activity will intensify.
have ended with a call for the development of a corporate law for cyberspace as a means to accomplish that regulation in a reasonable manner. This connection has been made before, in a different context and on the basis of different considerations. Curtis Karnow, for example, has suggested recognizing a new corporate entity in cyberspace, the e-person:

The corporation was molded to its modern form by extraordinary developments in trade and economics. I suggest the extraordinary developments in technology, and specifically the information, or digital, revolution, gives rise to a new legal entity: the electronic persona.

The new entity is bred between the anvil of free flow of information, and the hammer of security and privacy. As with the development of the corporate form, the central function of the new legal entity is simultaneously to (i) provide access to a new means of communal or economic interaction, and (ii) shield the physical, individual human being from certain types of liability or exposure.\(^6\)

For Karnow, legal recognition for e-persons is intimately connected with assuring privacy for those who act in cyberspace;\(^6\) I

---


\(^6\) Karnow writes:

Rights are conferred on epers for the same reason they are conferred on humans in the physical world: because there are powerful forces that we wish to restrain; and we cannot restrain those forces with countervailing raw power. We need a consensus that such raw power shall not ipso facto have its way. . . . [E]pers must be allowed some room, so that literal ownership of (i) the means of communication and (ii) agglutinated information does not thereby confer rights with respect to the content of the communication and the dissemination of the information. . . .

[E]pers are most useful when we need to communicate but still need a shield: when we want to maintain intact the ramified divisions of our social and economic lives. For privacy is not truly a matter of an absolute barricade; it is instead inhibiting the spillover of information from one place to another. . . . Here we find the central contribution of the eper. . . . Epers can provide the anonymity that this compelled exposure would destroy. Multiple epers can conduct business and—this is the point—keep information segregated. Epers are related only through the human progenitor, and that link can be encrypted. In a universe of utterly accessible mutating data, epers help ensure both access and privacy.

Id at 11-13. See also Mark A. Lemley, Rights of Attribution and Integrity in Online Communications, 1995 J Online L art 2 ¶ 40 (available online at
have tried to suggest that these e-persons have another role to play—facilitating collective action and creating reputational capital. E-persons have already begun to speak and act in online communities, notwithstanding (or, more likely, precisely because of) the fact that the legal system has paid them little mind, and we have only begun to understand the form that they may take or the values that they may embody—or the harms that they may cause. But we surely need to tread lightly in this area lest we, perhaps unintentionally, disturb the development of these most intriguing and potentially valuable arrangements.

http://www.law.cornell.edu/jol/jol.table.html) (cited in note 6) (discussing the need to protect pseudonymously named e-persons in order to protect the “virtual community” from damage).