1995

The Path of Cyberlaw

Lawrence Lessig

Recommended Citation
Lawrence Lessig, "The Path of Cyberlaw," 104 Yale Law Journal 1743 (1995).

The Path of Cyberlaw

Lawrence Lessig[†]

If you're not a cyberspace maven, but mill around a bit among those who talk about this cyberspace stuff—if you surf, as it is said, the information superhighway—there are two questions that you might ask about how this new space will get regulated.

The first question goes roughly like this: Should this new space, cyberspace, be regulated by analogy to the regulation of other space, not quite cyber, or should we give up analogy and start anew?[1] In Bruce Ackerman's terms, should we muddle into this new space as ordinary observers, just applying our old ways of thinking, or should we enter this world as scientific policymakers, armed with a comprehensive view, structuring the environment of this world to fit with this comprehensive view?[2]

The second question follows the first: Is cyberspace really anything new? Is there really a form of life here that we haven't known before, or is cyberspace just an electronic version of ordinary space, where the electronics might add something, but not really very much?

[†] Assistant Professor of Law, University of Chicago Law School <larry_lessig@law.uchicago.edu> The Sarah Scaife Foundation and the Russell Baker Scholars Fund provided support for this research. Thanks to Cass Sunstein for comments on a previous draft, and to an anonymous system administrator whose helpful and candid conversation helped me to begin thinking about this issue, and who warned me that if I "asked too many questions, there could be trouble."

[1] *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT L. REV. 993, 994 (1994) (discussing view that "old analogies just don't cut it").

[2] This schema is set out in BRUCE A. ACKERMAN, PRIVATE PROPERTY AND THE CONSTITUTION 10–15 (1977), as the product of two dimensions of opposition. The first dimension ranges between an ordinary versus scientific perspective on legal discourse and the second between an observer versus policymaking perspective. In the former, the ordinary perspective believes "legal language cannot be understood unless its roots in the ordinary talk of non-lawyers are constantly kept in mind" while the scientific believes that "the distinctive constituents of legal discourse [are] a set of technical concepts whose meanings are set in relation to one another by clear definitions without continuing reliance upon the way similar-sounding concepts are deployed in nonlegal talk." *Id.* at 10–11. By contrast, in the latter approach the observer believes "the test of a sound legal rule is the extent to which it vindicates the practices and expectations embedded in, and generated by, dominant social institutions" while the policymaker believes that the legal system contains "a relatively small number of general principles describing the abstract ideals which the legal system is understood to further." *Id.* at 11–12. The two dimensions together make four possible approaches—the ordinary observer, the ordinary policymaker, the scientific observer, and the scientific policymaker. Ackerman's focus in *Private Property* is on the two extreme ideal types of this matrix, the ordinary observer and the scientific policymaker. But as I suggest here, what is interesting about cyberspace regulation is the progression that it suggests through these four possibilities before one gets to the option of choosing between Ackerman's two types. One might, that is, need (epistemically) to pass through the ordinary observer stage to build a world within which scientific policymaking is possible. Or so I suggest here.

These two questions are interesting, I suggest, not just for what they will tell us about the regulation of cyberspace. They are significant too for what they will suggest about the regulation of ordinary space. For they will suggest what we must know, or where we must be, before we can regulate in ordinary space with a comprehensive view.

Consider the first question first: Will we regulate by analogy, or by something else? It should take just a second to see the strangeness in such a question. For just how could cyberspace be regulated except by analogy? Just what is it—cyberspace—apart from what we can describe by analogy? This is not a space that we know, in the sense of a space that we have inhabited. Indeed, in one sense, it is just a pattern of electrons skimming a net of computers, a construct that describes a location where a collection of activity occurs.[3] But described like this, the space could not be understood, or at least it could not be understood by us. It is understood by us only when we put things into it, when we carry into it our own language, when we colonize it, when we domesticate it. It is no accident that we speak of e-*mail*, or that we describe postings on "electronic *bulletin boards*," or that we wonder about the dynamics of real-time discussions in "CB-*chat*" areas. We have no choice but to take control of this space at first with our ordinary terms, if indeed we are to understand it. And it is through a practice of analogy that this occupation occurs.

The same point focuses the second question as well—whether there is really anything new here. For if we will understand this new realm at first by importing the old, then one way to understand the "new" is just that which does not fit old ways of speaking. The new will be that which we have to construct to describe—the gap between our old language and new experiences; the place where the ordinary observer's language gives out. We will discover what is new by applying, and failing to apply well, what is ordinary or old to this new space.

These two points suggest something important about how we should expect the regulation of cyberspace to proceed. For if the new in this new space is created as we use up the old, if we do not start with a world to regulate, but must build it, then what the system of cyberspace regulation will need is a way to pace any process of regulation—a way to let the experience catch up with the technology, a way to give the ordinary language a chance to evolve, and a way to encourage new languages where the old gives out.

This is the practice of the common law. But my plea here for the common law has little to do with common love for the common law: It is not because

[3] Its contours are actually far more complex. For an introduction to various conceptions of cyberspace, see Michael Benedikt, *Introduction* to CYBERSPACE: FIRST STEPS 1, 1–3 (Michael Benedikt ed., 1991).

the common law best reflects some truth about the nature of cyberspace,[4] or that the common law best reflects the customs of inhabitants of cyberspace,[5] or that the common law most efficiently orders the behavior of individuals in cyberspace.[6] What is special about the common law here is its constructive function. What recommends it is the process that it offers, with its partial answers, to repeated if slightly varied questions, in a range of contexts with a world of different talent and ideals. If, as Levi said, the common law is democratic, it is democratic not because many people get to vote together on what the law should mean, but because many people get to say what the common law should mean, each after the other, in a temporally spaced dialogue of cases and jurisdictions.[7] Unlike other lawmaking, what defines the process of the common law is small change, upon which much large change gets built; small understandings with which new understandings get made. What counsels it here is the way this process will function to create in an as yet uninhabited, unconstructed, world.

Thus in a sense what recommends the common law to cyberspace is not its efficiency, but its inefficiency. But to praise inefficiency, or better, a way to slow the regulation of cyberspace down, is not to say that cyberspace will need no regulation. Nor is it to say that we cannot yet see what the new here will be. In large part (I think) we can see what will be most important—what will be best—in this new space. What will be best ties directly to the questions addressed by this Symposium—associational and speech interests. To say that we need time to catch up is simply to note the extraordinary gap between what these associational interests are, or will be, and the world's present understanding of what exactly is at stake. Put another way, if we had to decide today, say, just what the First Amendment should mean in cyberspace, my sense is that we would get it fundamentally wrong.

What is this gap? Let me say something about what these associational interests will be, and something about the dark ages within which we now live. What is new, or to be consistent with myself, what will be new in this cyberspace stuff is not so much the new markets that this space will permit. They will be important, but they will not be importantly different from the markets we now know.[8] What will be new are the communities that this space will allow, and the constructive (in the sense of constructivist) possibilities that

[4] *Cf.* JOSEPH STORY, THE MISCELLANEOUS WRITINGS OF JOSEPH STORY 702 (photo. reprint 1972) (William W. Story ed., 1852) (discussing notion of common law as truth).

[5] *Cf.* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1870–1960, at 120 (1992) (discussing view of common law as custom).

[6] *Cf.* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 23–27 (4th ed. 1992) (discussing efficiency theory of common law); E. Donald Elliott, *The Evolutionary Tradition in Jurisprudence*, 85 COLUM. L. REV. 38, 63 (1985) (comparing evolutionary theories of law, including efficiency theory).

[7] EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 5–6 (1949).

[8] Eugene Volokh's account is an excellent prediction. *See* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995) (predicting future of music, print media, and video).

these communities will bring. People meet, and talk, and live in cyberspace in ways not possible in real space. They build and define themselves in cyberspace in ways not possible in real space. And before they get cut apart by regulation, we should know something about their form, and more about their potential.

We know enough to say a little about what these new forms of association are. They divide into three classes. The first we could call *association in public*. Here participants add to a common conversation, but with no real knowledge about who will read what they write. The best examples of these are postings to public bulletin boards. Usenet newsgroups are the most common on the net, where some 4000 different subjects are available for conversation,[9] and participants either add a new message within a topic or append a comment to comments previously made. While subjects are to be self-limiting, there is no formal mechanism for punishing those who violate subjects. Crossing subject borders may open one up to community sanction—flamings for violating rules of the Net[10]—but there are no Net police who make sure that the proper words fit in the proper place.

What results from this association is a dialogue of sorts, but one very different, I suggest, from dialogues that we now know. Like a town meeting, this is a dialogue contributed to by a wide range of people. But unlike a town meeting, because each response is appended to what went before, there is a relatively effective constraint to ensure that responses are responsive. Put another way, there is less return from being nonresponsive than in the drama of a town meeting. Moreover, because these dialogues go on over time and with relative anonymity, there is time for reflection and contribution from a wider range of participants than any single meeting would allow. Here is a place where discussion produces something, if indeed there is anything to produce.

A second form of association is more private. Call it an *association in private*. It functions like this: People link through the Net and chat (in real time) with others of their choosing (whether one or many) about a topic (or set of topics) of their choosing. What distinguishes this kind of association from the association in public is that this exchange is among known parties, and it lasts only so long as people are in the room. What is the same is that conversations are in texts, proceeding responsively.

Because the conversations here are (usually) in real time, the identity of the conversants is more significant. But identity is not fixed. Depending upon the service the participant gets to select whether he or she will be a she or he,

[9] Ethan Katsh, *Law in a Digital World: Computer Networks and Cyberspace*, 38 VILL. L. REV. 403, 431 n.53 (1993).

[10] "Flaming" is a verbal attack in cyberspace. On flaming, see John Seabrook, *My First Flame*, NEW YORKER, June 6, 1994, at 70; *see also* HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY 36–37 (1993) (discussing flame wars).

what he or she does, and so on. The chat room allows individuals a kind of individual plasticity—like a bar where you select your person before entering the room—and this plasticity allows individuals a kind of association unknown in real life. Here the ugly can speak seductively, or the shy can speak—period.

A third form of association mixes something of the last two, adding collective plasticity to individual plasticity. This we could call an *association in construction*. Like associations in public, these associations extend over time; but like the association in private, at any one time you know (again, as much as one can know) with whom you are associating, or more simply, playing. In this form, participants enter a virtual room, the structure and contents of which are subject to the community's control. The typical form is something called a MUD, or MOO,[11] where people not only speak, but they act, or more precisely, emote; where they not only engage in conversation, but also move around, where they touch, they assault, they construct. Players build the world within which they will then live, and these constructions survive over time, for others to play with or to change. This is a world where individuals not only are individually plastic, but a world where the world itself becomes plastic.

None of these forms of association is fundamentally new. (Again, how could they be?) Each has links with older analogs. The association in public is a kind of electronic town meeting; the association in private is a form of private club; the association in construction is a form of game or role playing made concrete in a virtual realm—Dworkin's chain novel, for the common man.[12] But however significant the similarities, we should see enough to know their potential to be something quite different. How different, how significant, we cannot yet quite see. We stand in relation to them as Alexander Graham Bell stood in relation to the telephone. Just as he, however visionary, could not have understood the idea of a "long-distance relationship," so too we will not yet understand the significance of these associations in cyberspace.[13] To understand them will require living them, in a world where these associations are real.

Thus there are these communities, nascent today, of possibly great potential tomorrow. Yet there is also an extraordinary blindness to this potential. The blindness comes in two forms, one from the techies who give us the machines upon which cyberspace gets built; and the other from the

[11] "MUD" stands for multiuser dungeon. RHEINGOLD, *supra* note 10, at 145. A "MOO" is a MUD, Object Oriented. Katie Hafner, *Get in the MOOd*, NEWSWEEK, Nov. 7, 1994, at 58–59.

[12] Dworkin's chain novel lives in RONALD DWORKIN, LAW'S EMPIRE 228–32 (1986).

[13] "When Alexander Graham Bell invented the telephone, he envisioned sending music over the wires. 'No one in their right mind, he thought, would tolerate something as intrusive as unannounced phone calls.'" Michael Antonoff et al., *The Complete Survival Guide to the Information Super Highway*, 244 POPULAR SCI., May 1994, at 97, 100.

regulators, who have their own special blindness to exactly what their regulation would take away.

First the techies: The same technology that will make possible this experiment in humanity can also, if allowed, destroy the very essence of what now defines individuality. I report here a conversation with the computer system administrator at a major university concerning information available to users about what other users at the university are doing on the computer system. As one can imagine, 7000 students and faculty members, plugged into the Net as they have been for a while, have begun to discover something of the potential that this world promises; they have begun to practice some of the forms of association I have just described. Most of this interaction is done through a UNIX-based machine.[14] UNIX offers users (ordinary users—I am not speaking of hackers) an extremely powerful ability to monitor just what others are doing. At any time, any user can type the command "w" at his or her (mainly his[15]) console, and the system will report what every other user of the system is doing at just that moment. On this listing, conveniently displayed for all to see, is an indication of, for example, with whom others are e-mailing, or with whom they are "chatting," or, more amazingly, what newsgroups they are reading. Hit the "w" command, and the system will report to you that user 123C is reading alt.politics.radical-left, or alt.sex.foot.fetish. And once you discover what 123C is reading, you can then use the "finger" function to discover who 123C is in real life, and then, using a phone book function, find out what 123C does, where 123C lives, and even when his or her birthday is.

If one can do this once, one can do it repeatedly. So that one could write a simple UNIX routine to scan the system every five minutes, and collect a profile of just what everyone is reading, to whom everyone is talking, and what everyone is thinking.[16]

[14] "UNIX" refers to the operating system of the machine, like DOS refers to the operating system of a primitive IBM PC, or Windows to the operating system of the more recent (and futile) efforts of Microsoft to mimic the Apple Macintosh. *Cf.* Andrew S. Rappaport & Shmuel Halevi, *The Computerless Computer Company*, HARV. BUS. REV., July–Aug. 1991, at 69, 71 (chronicling Apple/Microsoft competition).

[15] Peter H. Lewis, *Exploring New Soapboxes for Political Animals*, N.Y. TIMES, Jan. 10, 1995, at C6 (asserting most Internet users are male).

[16] Imagine you wanted to watch what user 123C was doing. The commands you would need are as follows. First, you would build a file called, for example, "check." The file would have the following lines in it:

```
date >> look.list
    w|grep 123C >> look.list
```

Each of these lines is a UNIX command. The first line executes a command that produces the date, and then puts it in the file "look.list." The second line executes the "w" command and then pipes the result through a filter (a function called "grep") that will extract all information related to 123C, and append it to the file "look.list." Finally, with a command called "crontab," you can set the "check" file to be invoked at anytime during the hour. Say you wanted to execute the command at the hour, and 15, 30, and 45 minutes past the hour. You would need the following entries in a crontab file:

```
00 * * * * check
15 * * * * check
```

I report this here—among lawyers, among people who for example have read *NAACP v. Alabama*[17]—because I trust this should be quite striking. Striking since no doubt very few of the users on the system actually realize that what they read, or with whom they speak, can so easily be monitored. And striking because the potential for abuse here, especially for vulnerable groups, is so great. Perhaps more surprising, however, was that the administrator with whom I spoke just couldn't understand the problem. I was, he said, the first person who had ever questioned the fact that this information was available to anyone and everyone. And the first person he had ever spoken to who even raised the possibility that there may be privacy issues at stake here.

The "techies" understand the potential of these forms of association, but it is as if they imagine associations of just techies—extremely smart, inquisitive, a bit counterculture, but deep down not such a bad lot.[18] They have known cyberspace longer than we have, but they imagine cyberspace populated by people other than us. The systems they have given us have extraordinary potential, but they were not designed to protect individuals against this extraordinary potential for others to abuse. The invasion of the "w" command is just one example of a more general problem[19]—the same technology that makes cyberspace possible also makes it extremely easy to monitor an increasingly large scope of individuals' lives.

The same technology, of course, can also help restore the privacy otherwise stolen. Two techniques in particular—in essence the same technique—allow users some ability to repurchase their privacy. One is the technique of anonymity, which enables individuals to control what about themselves is known by those with whom they interact—control, for example, whether others know a user's name or association or, more generally, any feature of that individual. The other is the technique of encryption, with which users are able, in effect, to speak a language that only intended recipients can understand. Both techniques are the same, for both are simply ways that the

```
30 * * * * check
45 * * * * check
```

So programmed, at 0, 15, 30, and 45 minutes after the hour, the program check would be run, and would search on the activity of 123C and pipe the results to the file look.list.

I am grateful to Larry Gryziak for outlining the routine for me. I include it here on the principle that it should exist only if most know about it, and in the hope that if most know about it (and others like it) it won't exist.

[17] 357 U.S. 449 (1958) (striking down statute requiring disclosure of membership lists as violative of Due Process Clause of Fourteenth Amendment and its protection of right to privacy of association). Of course the activity of the university in disclosing such information is not proscribed by *NAACP*. My claim is just that the interests that motivate *NAACP* should carry over to the university context.

[18] *But see* Gary Chapman, *Barbed Wired*, NEW REPUBLIC, Jan. 9 & 16, 1995, at 19 (describing antisocial, elitist attitude of techie culture).

[19] I don't mean to suggest that the function of the "w" command is necessarily problematic. In a world where people are not using machines for personal use, the command is legitimately useful. The problems begin once the machines enter aspects of life in which privacy is critical.

user can control what about him or her is knowable by others on the system, whether it be the user's identity, or the meaning of the words spoken. Both techniques give users the ability to recreate something of the privacy that the technology would otherwise have taken away.

The techniques of anonymity and cryptography themselves, however, have given rise to an extraordinary debate among legaloids. For both are getting to be far too good. Begin with anonymity. Given the range of associations that I have just surveyed (i.e., newsgroups, chat groups, and MUDs), we can see many good reasons why someone would want to remain anonymous or pseudonymous. One wants to contribute to a political discussion without suffering the cost of unpopular views; one wants to find information without revealing that one needs that information; one wants to assume a role in a certain discussion group to explore an alternative identity. All of these are relatively harmless (to society) uses of anonymity.

Not all anonymity, however, is so benign. Perfect anonymity makes perfect crime possible. The ability to appear invisibly on a network and slander, or harass or assault, certainly will increase the incidence of those on the network who slander, or harass or assault. Thus those who police worry that there may be real reason to prevent or regulate this technologically granted anonymity—to license it, or register it, to control how much about oneself one may not say.[20]

The same problem is raised by cryptography. As I have described it, cryptography is the ability not so much to hide who you are, but to hide what you say, by encoding it in a way that no one except intended readers can understand.[21] With public key encryption, it becomes extremely simple to make one's words truly private.[22] Then only with the proper key could someone unlock these thoughts.

The value of some encryption is the same as the value of some anonymity; indeed, it may be more pressing: a lawyer speaking to her client; two lovers on a public network; a purchaser sending credit card information over the Net. But the costs of encryption are also the same as the costs of anonymity: For just as there are perfectly good reasons why someone would want to hide her

[20] See, e.g., the proposal by Connecticut State Representative Pat Dillon "that would virtually eliminate anonymity on-line." Beverly Galge, *The Babe File*, NEW HAVEN ADVOCATE, Feb. 9, 1995, at 7; *see also* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709, 742–43 (1995) (discussing government positions on encryption).

[21] For an extraordinarily complete account of this debate, see Froomkin, *supra* note 20.

[22] With public key encryption, messages require two keys to be decrypted, one public key, and one private key. With the public key, a user can encrypt a message that then can be read only by the holder of the private key. *See* EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 30 (1994); BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE 17 (1991). So, for example, a hitman could advertise his willingness to commit some crime, and publish the ad with his public key. Then, someone could accept the offer, encrypting the acceptance with the public key, and be assured that only the hitman could read the acceptance. A separate problem, however, is whether the offeree can tell if the offeror is who he says he is.

or his words from unwanted eyes, there are perfectly evil reasons why someone would want to do so. Again, encryption makes possible criminal activity (a conspiracy) without any possibility of the government tracking it down.

One should not exaggerate the government's or society's loss here. No doubt it has always been possible for people to find places where their words can be understood only by the intended recipient. An encrypted conversation is just the 1990's version of a walk in the park, or a chat on the subway. But even unexaggerated, the government's fear here is real: With perfect encryption or perfect anonymity, the return to crime certainly does increase. And this increase certainly does justify the government's interest in finding ways to regulate both.[23]

[23] To date, the government's policy with respect to encryption has been to assure the success of its own encryption technology—the Clipper Chip—which provides encryption for voice communication while providing a back door with which the government can listen to the conversations it believes it must listen to. Clipper has excited an extraordinary reaction in the cybercommunity, the vast majority of it passionately devoted to stopping Clipper. NATIONAL RESEARCH COUNCIL ET AL., RIGHTS AND RESPONSIBILITIES OF PARTICIPANTS IN NETWORKED COMMUNITIES 25 (Dorothy E. Denning & Herbert S. Lin eds., 1994); *see* Froomkin, *supra* note 20, at 798 & n.371; *see also* CAVAZOS & MORIN, *supra* note 22, at 31 (noting that Clipper Chip is controversial). The aim, the cybercommunity worries, of the government's policy is to assure that the only encryption technology out there is the government's, which, the cybercommunity worries again, means that the government will be in the position to listen to whatever conversations it chooses.

Subject to two important qualifications, I confess that I don't quite get the fear. If every telephone in America had a Clipper Chip on it as of tomorrow, there can be no doubt that net privacy in America would increase. Froomkin, *supra* note 20, at 742–44. For today, the vast majority of conversations are not encrypted, which means that today, anyone (whether government or not) can tap into and understand most of what is being said. If Clipper were on every phone, then the only people who could listen to telephone conversations would be those who have, or could break, the Clipper code. No doubt that since the government controls the Clipper code, this would tilt the balance among eavesdroppers clearly in the government's favor. But so what? While it would be easier for the government to eavesdrop than for my neighbor or competitor or enemy, it still would be extremely hard for the government to eavesdrop *illegally*. More precisely, it still would be much more difficult than it is today for the government to eavesdrop illegally, which would, one should think, decrease the amount of illegal governmental spying, while nearly eliminating illegal private spying.

What the opponents of Clipper really oppose is a government monopoly on encryption technology—both because of a (legitimate) fear that the technology of Clipper is not very good, and because of the concern that only the government holds the keys. This latter concern again seems exaggerated. Even if every phone had Clipper, one could still encrypt the conversations that the Clipper Chip would then encrypt again—double encryption, that is. And while the government might someday want to ban this double encryption, this possibility seems remote, not only because democrats abhor a government monopoly, but also because it just seems so technically infeasible. *See id.* at 795, 808. In any case, that seems to be a battle that should be fought on its own terms, not fought in the context of government support for a technology that will on balance increase individual privacy. That, it seems to me, is just what Clipper now is.

As I said at the start, however, there is good reason to be concerned about this particular encryption regime. As Michael Froomkin well outlines, *id.* at 764–93, the present regime provides no real protection against the improper release of escrowed keys. As he explains, there is, first, no structural assurance that the Executive could not evade the limitations on access to the keys, and second, no guarantee that a second copy of all keys is not being held by, for example, the National Security Agency. Assurance against the second concern is not easy to give. Assurance against the first would exist if, for example, one-half of each key were given to the judicial branch to hold, to be released only upon the issuance of a warrant. Froomkin argues this would violate principles of separation of powers, *id.* at 783–85, because it would be imposing nonjudicial duties on judges—a violation of the *Hayburn's* principle. This is, I believe, a mistake. Requiring that the judicial *branch* hold the keys is distinct from requiring *judges* to hold the keys. All sorts of duties

With both, a constitutional balance will have to be drawn between these increasingly important interests in privacy, and the competing interest in collective security. Already the extremes are well staked out, with some arguing that no regulation of either should be permitted, and others arguing that only with regulation should either be allowed.[24]

My point, however, is not about what the balance should be.[25] My point is about timing—when the balance should be drawn. There are many who now see the extraordinary expressive and associational potential that cyberspace offers. Most, however, do not. If the many prove correct, the most will eventually see the same—as the space becomes more common, as their children become transformed by it, as life takes root within it. But this seeing will take time. It will require that individuals gain an experience with this new space that gives them the sense of what this new space is. Only when this experience is common should we expect to be in a position to understand its significance. When the technology, when the experience, when the life in cyberspace presses us, only then should we expect law to understand enough to resolve these questions rightly.

To meet this point about timing, I have suggested that we follow the meandering development of the common law. Let me end by returning to this theme in the specific context of the First Amendment, to ask how, just now, First Amendment doctrine should respond.

My suggestion is that it shouldn't. Or at least it shouldn't just now. Or at least it should do everything it can to stand back from deciding these conflicts until the nature of these conflicts is well mapped, well constructed, well understood. A prudent Court—Supreme Court, that is—would find ways to let these questions simmer for a while, to let the transition into this new space advance, before venturing too boldly into its regulation. Not that no court should decide these issues—for again, there is a great value and an important need for lower courts to wrestle with these questions, if only to create a body of legal material from which others may draw in considering these questions.

are imposed on inferior officers in the judicial branch by Congress and judges without anyone thinking this violates the *Hayburn's* principle. For again, it would be these officers, not the judges, who would administer the keys, and who would release the keys when a judge issued a warrant. With respect to the judges, then, giving the keys to the judicial branch would not change their responsibilities at all, but with respect to the President, because officers in the judicial branch are responsible to someone other than the President, it would help ensure that keys are not improperly released.

The second concern about the existing regime is the increasing problem of call identification. What was called pen register information will become much more easily accessible. Pen register information tracks who called whom when. Given the multiplicity of ways in which people call others (phones, e-mail, fax), this becomes an increasingly invasive exception to privacy norms. *See id.* at 762 n.211.

[24] See the collection of positions in 1994 CRYPTOGRAPHY AND PRIVACY SOURCEBOOK (David Banisar ed., 1994).

[25] Of course, I have my own view. I can see nothing wrong with requiring that all systems attach encrypted fingerprints on all transactions, such that it is always possible, with a key, to trace a transaction back to a particular individual, though impossible, without the key, to decrypt the fingerprint to identify that person.

But no court should purport to decide these questions finally or even firmly. Here especially should be the beginning of a dialogue, which perhaps more than others is meant to construct its subject more than reflect it. And since it is easier to correct lower court mistakes, or second-guess lower court intuitions, it is at this lower level that the dialogue should occur. Constitutional law is fundamentally concerned with who should decide what constitutional questions when. My suggestion here is that we rely for the moment on lower court judges, to give the law the material with which to understand this new realm.

The point should be especially salient at Alex Bickel's Yale.[26] It may already be latent in the Court's most recent venture close to the boundaries of cyberspace and the First Amendment, *Turner Broadcasting System, Inc. v. FCC.*[27] In my view the most important passage in *Turner* comes right at the beginning, where Justice Kennedy writes:

> The role of cable television in the Nation's communications system has undergone dramatic change over the past 45 years. Given the pace of technological advancement and the increasing convergence between cable and other electronic media, the cable industry today stands at the center of an ongoing telecommunications revolution with still undefined potential to affect the way we communicate and develop our intellectual resources.[28]

Exactly. And what should follow from this "undefined potential" is lots of room for democratic experimentation. Experimentation, because stable doctrine is only built upon the ground of long-standing experimentation. What any review of the history of First Amendment law should suggest is the contingency of present First Amendment doctrine.[29] For most of its history, the amendment had nothing of the bite that it now has. For most of its history, it was little more than an aspiration, rarely latched onto by the courts to limit the democratic (or not so democratic) branches.[30]

Somehow this legal culture got beyond that contingency, and fortunate for us that it did. Though we live in a post-realist, post–New Deal age, there is little impatience in First Amendment law with formalisms that other domains of constitutional law could not account, and little hesitancy in First

[26] Best exemplified in ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH (1962).

[27] 114 S. Ct. 2445 (1994).

[28] *Id.* at 2451.

[29] *See, e.g.*, Jamie Kalven, *Editor's Introduction* to HARRY KALVEN, JR., A WORTHY TRADITION at xi, xxxi (1988) (discussing relative fragility and vulnerability of First Amendment doctrine); Steven L. Winter, *Fast Food and False Friends in the Shopping Mall of Ideas*, 64 U. COLO. L. REV. 965, 973 (1993) (discussing "social contingencies" upon which First Amendment law rests); David Yassky, *Eras of the First Amendment*, 91 COLUM. L. REV. 1699, 1742–44 (1991) (arguing First Amendment's strength did not develop by "gradual progress," but rather "burst out of nowhere").

[30] *See* KALVEN, *supra* note 29, at 167, 459–61.

Amendment law to interfere with democrats in the name of the values these formalisms manifest.

We should take note of this anomaly, stand back from it in a bit of post-realist awe, and then be very careful to understand the conditions under which this judicial power has been made possible, and careful about how much of a burden we can expect this amendment to bear. Already we can see the structure slowly being drawn into question. Hate speech and pornography regulations are forcing into the foreground the presuppositions that had cemented the formal structures of First Amendment law in the first place.[31] These challenges may succeed in dislodging the dominant mode of analysis. But until they do, we should move slowly in applying the First Amendment elsewhere.[32]

Cyberspace is elsewhere, and before carving the First Amendment into its silicon, we should give the culture a chance to understand it. By "we," again, I mean the Court. A prudent Court would let these issues evolve, long into this revolution, until the nature of the beast became a bit more defined. If there is sanction to intervene, then it is simply to assure that the revolution continue, not to assure that every step conforms with the First Amendment as now understood.

Turner suggests there may be such room, though I am not as optimistic as Cass Sunstein[33] that the room left is indeed very broad. What the Court should do when turning *Turner* on cyberspace proper is mark out the deference even more clearly. While the nature of the domain is so fundamentally contested, no clear command from the Court should be heard.[34] Instead, while

[31] *See generally* CATHARINE A. MACKINNON, ONLY WORDS (1993) (discussing defamation, harassment, and equality in light of First Amendment doctrine); CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH (1993) (describing "hard cases" in First Amendment jurisprudence, including hate speech and pornography); Akhil Reed Amar, *The Case of the Missing Amendments:* R.A.V. v. City of St. Paul, 106 HARV. L. REV. 124 (1992) (articulating role for Thirteenth and Fourteenth Amendments in hate speech debate); Frederick Schauer, *Exceptions*, 58 U. CHI. L. REV. 871, 886–91 (1991) (discussing hate speech and pornography).

[32] To say that we should move slowly makes it sound as if there is an unregulated world, one that is slowly getting regulated. This is of course false. Cyberspace is regulated everywhere, and its current faddish appeal will no doubt ensure more legislative regulation. Why not, then, the regulation of the First Amendment? Or, more precisely, why not apply the anti-regulatory judicial power of the First Amendment to limit current efforts at legislative regulation? One answer would point to the unruliness of judicial rules and the unintended consequences of regulation, especially in a world not well understood. *See, e.g.*, EUGENE BARDACH & ROBERT A. KAGAN, GOING BY THE BOOK: THE PROBLEM OF REGULATORY UNREASONABLENESS 58–92 (1982). My argument, however, is more about timing and the relative plasticity of Supreme Court precedent. The scope of judicial protection cannot help but be affected by the common understanding of the nature of cyberspace. A lack of common understanding will skew this influence. And because the Court is relatively slow to revise its precedent, this skewing effect may be a significant block in cyberspace's development. The following comparison may make the point: If the Supreme Court cannot yet understand the social meaning of the modern American airport, *cf.* International Soc'y for Krishna Consciousness, Inc. v. Lee, 112 S. Ct. 2701 (1992) (holding that airports are nonpublic fora), is there reason to expect that it will understand the social meaning of cyberspace?

[33] *See* Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1779–80 (1995).

[34] I discuss the relationship between contested domains of thought and the possibility of judicial authority in *Understanding Changed Readings: Fidelity and Theory*, 47 STAN. L. REV. 395, 438–42 (1995).

the nature of this domain is contested, the Court should find ways to let the contest resolve itself. There will be time enough for principle when the dealing, associational or not, is done.