45 Emory L.J. Number 3 (1996)

READING THE CONSTITUTION IN CYBERSPACE

Lawrence Lessig[†]

We might distinguish between two types of constitutional regimes, one codifying, the other transformative. A codifying constitutional regime aims at preserving something essential from the then-current constitutional or legal culture—to protect it against change in the future; a transformative constitutional regime aims at changing something essential in the then-current constitutional or legal culture—to make it different in the future. The picture of the codifying regime is Ulysses tied to the mast; the picture of the transformative is revolutionary France.

In our constitutional tradition, the Constitution of 1791 was a codifying constitution—the Bill of Rights, that is, was a constitutional regime that sought to entrench certain practices and values against change.[1] The Civil War Amendments, on the other hand, were transformative, aiming to remake something of what the American social and legal culture had become, to tear out from the American soul its tradition of inequality, and replace it with a practice of equality.[2]

[†] Professor of Law, University of Chicago School of Law. Thanks to the ever-present Chicago roundtable, as well as Bruce Ackerman, Tracey Meares, and Judge Richard Posner, for helpful advice. Funding for this project was provided by the Russell Baker Scholars Fund and the Sarah Scaife Foundation. Thanks also to Ashley Parrish for the exceptional work that is his norm.

[1] *See, e.g.*, JACK N. RAKOVE, ORIGINAL MEANINGS: POLITICS AND IDEAS IN THE MAKING OF THE CONSTITUTION 302 (1996). *See also* Akhil Reed Amar, *The Bill of Rights as a Constitution*, 100 YALE L.J. 1131 (1991), for another such understanding of the Bill of Rights.

[2] This is not to deny that there were aspects of the equality in the Civil War Amendments that echoed in our constitutional past. The abolitionists, of course, made great weight of the Declaration of Independence's claims to equality. *See, e.g.*, Trisha Olson, *The Natural Law Foundation of the Privileges or Immunities Clause of the Fourteenth Amendment*, 48 ARK. L. REV. 347, 364 (1995). But

One might well be skeptical of transformative constitutionalism generally. One could be skeptical enough about our own transformative past, let alone of the prospects for some of the more prominent transformations in post-communist Europe. In this essay, however, I will be skeptical of codifying constitutionalism. And I am skeptical here at a conference about cyberspace because cyberspace will make plain just how difficult a practice codifying constitutionalism really is.

We might think of the problem like this: A codifying constitution enacts a set of legal constraints on (in our tradition) governmental action.[3] But these constraints are just one kind of constraint on governmental action. The other we might call the constraints of technology. The warrant requirement is a legal constraint on police action; that the police, unlike Superman, don't have x-ray vision is a technological constraint. We don't think much about technological constraints when thinking of the constraints of law. We usually just take them for granted. But we should. For what draws into doubt codifying constitutionalism is just what happens when these constraints of technology change, or more importantly, when we have the power to change them.

The Fourth Amendment is a ready example. At the time of the founding, the technologies for invading an individual's private space were few. There were spies, eavesdropping and listening through windows or doors; but all these are fairly costly technologies, meaning that the ability to live free of review within the confines of one's home was fairly strong. This is not to say that life at the framing was more private—certainly neighbors were more nosy, and certainly most of one's life was more public.[4] But within one's home, or one's own papers, the ability of the state to monitor what was going on was quite slight and crude.

The common law of trespass and the protections of the Fourth Amendment rested upon this fairly crude technology of surveillance. They supplemented these technological constraints with legal constraints. The common law of trespass made it an offense for anyone to cross over into my property; the Fourth Amendment made it an

---

an amendment can be transformative even if it is simply recalling a part of the past, and reestablishing it. This, for example, is what Germany did after World War II.

[3] Other constitutional regimes, of course, have been understood to restrain more than governmental action. Germany is a prominent example. *See* DAVID CURRIE, THE CONSTITUTION OF THE FEDERAL REPUBLIC OF GERMANY 182-83 (1995).

[4] *See, e.g.*, RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 268-71 (1981).

offense for a (federal) officer to escape the proscriptions of the common law, unless that officer had either a warrant, or the search was, under the circumstances, reasonable.[5] Without a warrant, or without sufficient cause, an officer of the state was liable in damages for the trespass. This liability strengthened the protection of privacy beyond protections of the technological constraints.

These technological and these legal constraints combined to define the constraints that confronted the state as it desired, if it desired, to intrude into a citizen's private domain. The sum of these constraints, both legal and technological, might be said to define the domain of security that the individual had against such intrusion.

Now it is a commonplace that a constitution, at least a codifying constitution, is to preserve these legal constraints against the changes of time. It is a commonplace, that is, that a court's task is to assure that framing values of dignity[6] and liberty are maintained, passions for "law and order" notwithstanding. It is a commonplace, though, in the context of the Fourth Amendment, that is increasingly ignored.[7] But whether respected in practice or in the breach, at least our ideals are clear—at least we are clear about what we are supposed to do. About legal values that the Framers constitutionalized, we are to be firm: preserving them against the changes in passions that later generations might bring.

But what should we do about changes in technology? What is a court to do when technologies make it easier for police to monitor what happens inside the home? Or when technologies make it easier for citizens to hide? Here the question is more difficult, and we have at least one clear example of two very different responses.

The case is *Olmstead v. United States*,[8] and the question was whether wiretapping was within the scope of the Fourth Amendment. The Court held it was not. When the Constitution was enacted, said Chief Justice Taft, the Fourth Amendment was intended to limit trespass on property; that was the common law origin of the

---

[5] TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 21-50 (1969); Amar, *supra* note 1, at 1178-80.

[6] Minnesota v. Dickerson, 508 U.S. 366, 380-83 (1993) (Scalia, J., concurring).

[7] *See, e.g.*, Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1 (1994).

[8] 277 U.S. 438 (1928). *See also* JAMES BOYD WHITE, JUSTICE AS TRANSLATION 149-57 (1989).

Amendment. Wiretapping a person's phone is not a trespass; therefore, concluded Taft, wiretapping did not invade the Fourth Amendment's interests.

Justice Brandeis saw the case differently. Of course the Fourth Amendment originally protected against trespass, but this was because trespass was the only effective way that the state could invade privacy interests.[9] Sure, it could eavesdrop without trespassing, so it could in some sense intrude without constitutional violation; but eavesdropping was of little importance at the founding since police were nonexistent, and eavesdropping quite public. And in any case, eavesdropping is not as significant an invasion as the invasion that would be permitted if the government could tap phones without limit. For even in 1928, much of life had moved onto the wires; and in those first steps into cyberspace, Brandeis argued, the Constitution should not leave citizens exposed.[10] What had changed, he argued, was a technology of surveillance and a technology of communication.[11] Life existed now in cyberspace, and the Constitution should be read to protect the same interests of privacy in cyberspace that the Framers had protected in real space. Technology had changed, but, Brandeis argued, that change should not be allowed to change the meaning of the Constitution.[12] The Constitution should protect now what it protected then.

If there is a Justice who deserves c-world's praise, if there is an opinion of the Supreme Court that should be the model for cyberactivists, if there is a first chapter in the fight to protect cyberspace, it is this Justice, this opinion and this case. Here, in as clear an example as any, is a method that will be central to cyberspace's survival as a place where values of individual liberty are sustained. The

---

9 As Brandeis wrote, "When the Fourth and Fifth Amendments were adopted, the form that evil had theretofore taken had been necessarily simple." 277 U.S. at 473.

10 The amici curiae from the telephone companies in the *Olmstead* case presented quite effectively the place the telephone had taken in the ordinary life of most citizens. See Brief in Support of Petitioners' Contention, on behalf of Pacific Telephone and Telegraphy Co., et al., *Olmstead*, 277 U.S. 438.

11 277 U.S. at 473.

12 Brandeis's fears were well stated: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Id.* at 474.

method is *translation*:[13] Brandeis first identifies values from the original Fourth Amendment, and then *translates* these values into the context of cyberspace. He read beyond the specific applications that the Framers had in mind, to find the meaning they intended to constitutionalize. He found a way to read the Constitution in 1928 to preserve the meaning it had in 1791. Brandeis's opinion shows how to carry the Framers' values into our interpretive context, in a way that has an extremely strong claim to constitutional fidelity. The argument was as simple as it was compelling: By doing what the Framers would have done, Brandeis argued, the Court would change the Constitution's meaning (since now a large part of intimate life was open to governmental intrusion without the protections of the Fourth Amendment); and by doing something other than what the Framers would have done (by protecting something more than trespass), the Court could preserve the Constitution's meaning.

In the almost seventy years since Brandeis's opinion, we haven't any better example of the translator's craft. Unlike originalists who believe that fidelity requires doing just what the Framers would have done,[14] the translator understands that to preserve meaning across contexts, one must change readings across context.[15] This is what the linguistic translator does: In Germany, she says "danke." In France, she says "merci." In the two places she has said different things, but in both places, she has meant the very same thing. Contexts are different, so meaning is preserved by saying something different.

The most cyberspace could hope for, from judges at least, is the practice that Brandeis offered; the most we could aspire to, in interpreting our Constitution, is the sensitivity that he displayed. But in this Article, I want to point to the limits of even this method of interpretive fidelity. Translation may well be fidelity's best method; but

---

[13] Paul Brest, *The Misconceived Quest for the Original Understanding*, 60 B.U. L. REV. 204, 218 (1980). For a recent application, see William Michael Treanor, *The Original Understanding of the Takings Clause and the Political Process*, 95 COLUM. L. REV. 782 (1995). See generally Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993); Larry Alexander, *All or Nothing at All? The Intentions of Authorities and the Authority of Intentions*, *in* LAW AND INTERPRETATION: ESSAYS IN LEGAL PHILOSOPHY 371-75 (1995); and RICHARD A. POSNER, OVERCOMING LAW 494-97 (1995) for useful criticism of the method.

[14] This we might call "one-step" originalism. *See* Lessig, *supra* note 13, at 1183-85.

[15] And this we might call "two-step" originalism. *Id.*

my argument here is about how difficult fidelity in cyberspace is going to be.

The point is this: We, as a legal culture, want the Constitution to resolve the questions of rights; we don't want them to be in the center of our interpretive struggles. We therefore seek, through various forms of originalism, ways to link our constitutional practice today to the practice of the Framers. We seek the authority of originalism, as a trump in present legal disputes, and the best way to locate that authority is Brandeis's—translation.

But even the best translations at some point give out. Even the most careful translators must at some stage concede there is not enough left from the framing regime to guide any more.[16] Translation will have its limits, and these limits will be of great and, I fear, terrible significance for us today. For what these limits will yield is a relatively passive judiciary, and a relatively deferential attitude toward governmental intrusion. My sense is that, knowing nothing, or at least not very much, terrified by the threats of that which they don't know, these judges will defer to those with democratic authority; without clear rules to limit the democrats, the juricrats will step aside.

One can hardly blame them for this. Indeed, in some cases this deference should be encouraged.[17] But I want to move that counsel of prudence along a bit—to place it in context and limit its reach. We should understand just why the judge's position will be so difficult and we should isolate the source of the difficulty. In some places, this difficulty should counsel deference, a certain hesitation before resolving the questions of the Constitution in cyberspace finally, or firmly, or with any pretense to permanence. But in others, I argue that judges—especially lower court judges—should be stronger. In cases of simple translation, judges should advance quite firmly arguments that seek to preserve original values of liberty in a very different context. In these places, there is a space for activism. But in cases where translation is not so simple, judges should kvetch. In these places, they should talk about the questions these changes

---

16 Felix Cohen, *Field Theory and Judicial Logic*, 59 YALE L.J. 239, 272 (1950) ("Only in mathematics do we find perfect translations—the sort of thing that enables us to translate any proposition about a straight line in Euclidean geometry into an equivalent proposition about a curve in Riemannian geometry. But outside mathematics, though we live in a world of imperfections, some imperfections are worse than others.").

17 One could well have argued that during the crisis of the Depression, deference by the Court to the Congress was well advised. *See, e.g.*, CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH 39 (1993).

raise. And if the result is deferential or passive, it should be so in protest. Here there may well be a place for prudence in deed, but to earn this right to be passive, to compensate for allowing rights claims to fail, judges should not be deferential in word. They should raise before the legal culture the conflict that these new cases present. Hard cases need not make bad law; but neither should they be treated as if they were easy.

This Article moves in two stages. I begin with some examples of the changes that cyberspace will present, and some of the questions of constitutionalism that these changes will invite. Following Brandeis, in each case I hazard a translation that reflects what I believe is the best guess at the most we could expect a court in such a case to do. That is Section I.

In Section II, I will isolate what about these changes makes them so significant, and what about them makes the change of cyberspace itself so significant, at least to the practice of constitutional fidelity. In a line that will no doubt seem far too abstract, we might describe the problem of cyberspace for constitutional law like this: That it leaves us without constraint enough; that we are, vis-à-vis the laws of nature in this new space, gods; and that the problem with being gods is that we must choose. These choices will be choices of great moment; they will raise contested values; they will be of great constitutional significance; but they will be made by an institution that is, as it were, allergic to such choice. They will be made, by a Court, pretending that in making its decisions, it is following the choice of others—of the people, of "we the people," who in truth have not yet confronted the constitutional choices that must be made.

I. THREE PROBLEMS FROM CYBERSPACE

I begin with three puzzles presented by cyberspace, and something of the constitutional issues that they raise. I then attempt to solve these puzzles using the technique of translation. My treatment of each, of course, will be far less extensive than a complete account would have to be. But my point in presenting the three is not finally to answer them, but rather to draw out from the collection something important and general about cyberspace.

Anonymity

The architecture of cyberspace—as it is just now—is open.[18] One enters cyberspace as one wants. One can enter identifying who one is, or one can hide who one is. One can enter speaking a language that anyone can understand, or one can encrypt the language one speaks, so only the intended listeners can understand what one says.[19] What others see of you is within your control; whether others understand of you is within your control as well.

We can call this general power of control a power of privacy.[20] It is the power to determine what others will know about you; the power to determine whether they will know your name, or who you are; the power to determine whether they will know what you say, or even what language you speak. Anonymity refers to the power to control whether people know who you are; it is a tool of privacy. Encryption is the power to control whether people know what language you speak; it too is a tool of privacy.

To some degree, technologies of privacy exist everywhere in real life. If one wants to hide who one is, one can don a mask, or use a fake name. One can speak in code, or in a language that very few understand. Not many people do, of course. The streets are not filled with masked men, and it is actually quite difficult to use a fake name. But nonetheless, since espionage began, there have been techniques for appearing as other than who one is, and people have used these techniques to construct a certain personal anonymity.

But anonymity in cyberspace is not just different in degree from anonymity in real space. As cyberspace presently is, it gives an individual a kind of power that doesn't exist in real space. This is not just the ability to put on a mask; it is the ability to hide absolutely

---

18 I am following Monroe Price in this distinction. *See* Monroe Price, *Free Expression and Digital Dreams*, 22 CRITICAL INQ. 64, 67 (1995). It is this architecture of openness that makes possible the world Tim May describes as crypto-anarchy. *See* Timothy C. May, Crypto-Anarchy and Virtual Communities, Posted to Cypherpunks List, December 1994.

19 On the technologies of encryption, see A. Michael Froomkin, *The Metaphor Is the Key: Cryptograph, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); U.S. Cong. Off. Techn. Assessment, *Information Security and Privacy in Network Environments*, 111-32 (1994). On the constitutionality of government control of encryption, see Froomkin, *supra*.

20 *See* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 44-45 (1994); OSCAR GANDY, THE PANOPTIC SORT 190 (1993); M. ETHAN KATSH, LAW IN A DIGITAL WORLD 228 (1995); M. ETHAN KATSH, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF LAW 189-97 (1989). *See also* JEFFREY ROTHFEDER, PRIVACY FOR SALE (1992); ALAN WESTIN, PRIVACY AND FREEDOM (1967).

who one is. It is not just the ability to speak a different, or encoded, language; it is the ability to speak a language that is (practically) impossible to crack.[21] Cyberspace is a place that maximizes both social and individual plasticity, which means it is a place that determines very little about what others must know about you.

This power of privacy is not inherently bad.[22] Indeed, one way to understand its salience is as a reaction to just the opposite trend. As the powers of surveillance have increased (through sophisticated transaction tracking devices that can collect profiles of individual behavior and predict future behavior on the basis of these profiles), one might well understand the anonymity as a effort at reclaiming private space lost. As the number of eyes that watch increase, anonymity becomes a more effective technology to block the vision of any one set. So understood, these tools of privacy are accommodations to the increased power of surveillance that the changing technologies of surveillance have created.[23]

The most important place for this technology will be commerce.[24] There was a time when we relied upon another tool of anonymity to a very large degree: cash. Cash is an almost perfect tool of anonymity. Nothing in its nature reveals anything about the person using it; it is self-authenticating, depending upon individual credentials not at all. One could use cash, and unless identification were independently given, the identity of the one who used the cash would be lost to the system. Cash flows without a trace.

---

21 There is in fact an ongoing question about whether these algorithms can be cracked. *See* Froomkin, *supra* note 19, at 735-42. Levy describes an example where the Internet facilitated a conspiracy to crack a code, with great success. *See* Steven Levy, *Wisecrackers*, WIRED, Mar. 1996, at 128. Where this struggle ends is yet undetermined.

22 *But see* RICHARD A. POSNER, OVERCOMING LAW ch. 25 (1995).

23 *See* STEVEN L. NOCK, THE COSTS OF PRIVACY 1-14 (1993). For a general and extremely helpful discussion of privacy in cyberspace, see Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63 (1995).

24 *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996).

Digital cash[25] is the next great cash station.[26] Digital cash, like regular cash, can be traded without traceability.[27] Giving digital cash to another creates a credit in their account without any traceable liability to the giver. More importantly, such transfers can occur without the most common burden of cash getting in the way—the risk of loss. One can move $1,000,000 in digital cash with just the touch of a button; one can move $1,000,000 in regular cash only with a wheelbarrow.

But when one begins to think of digital cash, and then encrypted conversation, and when one puts the two together, one begins to see the fear this very same power of anonymity creates.[28] For anonymity becomes a technology for the perfect crime.[29] And the question then becomes whether there is an ability—let's start and stop with constitutional permissibility—to regulate this anonymity.

What kind of regulation would this be? It would certainly be too broad to ban all encrypted conversation.[30] Indeed, there may well be a constitutional right to encryption, as a constitutional accommodation to the paucity of constitutional protection for personal informa-

---

25 Private money has a long history in America; *see* VIVIANA A. ZELIZER, THE SOCIAL MEANING OF MONEY (1994). One might wonder to what extent the government will allow competing currency to return.

26 *See, e.g.*, KEVIN KELLY, OUT OF CONTROL 203-30 (1994).

27 I am talking about what is technologically possible, not what is technologically necessary. Indeed, my central point is that there is very little that is "necessary" and too much that is possible.

28 For an excellent discussion of legal dilemmas related to these questions, see Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995).

29 *See* Froomkin, *supra* note 19, at 727; BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE 323-91 (Lance J. Hoffman ed., 1994). For a more immediate concern about the negative consequences of anonymity, see *McIntyre v. Ohio Elections Comm'n*, 115 S. Ct. 1511, 1537 (1995) (Scalia, J., dissenting).

30 This has not stopped some states from trying. *See* 18 PA. CONS. STAT. § 910 (Supp. 1996) (Pennsylvania statute making it a crime to possess a program or device which can be used to "conceal or to assist another to conceal the existence or place of origin or of destination of any telecommunication"). *See also* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 n.20 (1995) (Connecticut bill).

tion held in public space.[31] Contract notwithstanding, the data about me collected by others, or the data of mine that I put in public space, is open to government theft without fear of constitutional penalty.[32] This means that as the technologies of data collection and use have advanced, the extent of my privacy has declined, just because the extent of information held about me in public space has changed: Whereas before I might have lived ninety percent of my life in places essentially protected from government surveillance, now I live ninety percent of my life in a place completely open to government surveillance. Encryption may just be the technological accommodation needed to balance this technological loss of control.

But what about a lesser regulation? Imagine that the government banned any encryption technology that was not registered, in the sense that it preserved in its design a "back door,"[33] so that government officials could decrypt a conversation if they had proper authorization.[34] Of course, for good David Post-like reasons,[35] this could not be a successful regulation if simply imposed as a rule (the Net spits out mandates); and of course, there is no simple way to describe what any such system would be, since there are many ways a system could implement this type of back-door access. But assuming that we could get the system implemented, and assuming

---

31 *See, e.g.*, Jill M. Ryan, Note, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption,* 4 WM. & MARY BILL RTS. J. 1165 (1996).

32 *See* United States v. Miller, 425 U.S. 435 (1976). For a compelling (and depressing) account of the constitutional protections for "interpersonal privacy" see Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment,* 4 N. ILL. U. L. REV. 1 (1983).

33 A "back door" provides access to a system through a route other than one designed for primary users.

34 The possibilities here are many. *See* A. Michael Froomkin, *The Constitutionality of Mandatory Key Escrow, in* BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE, *supra* note 29, at 413.

35 David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace,* 1995 J. ONLINE L. art. 3 (1995). Post argues that because the Net facilitates easy exit, "rule-sets" imposed by governments will be easily evaded. Thus the techniques of regulation cannot be the direct techniques of prohibition, but must use market regulation as the means. This is an extremely important argument, and article, and I agree with the general point it is making. But the extent of the flexibility depends upon the technology. At this stage, the more radical point that Post makes has not yet been reached.

that we could select a sufficiently secure system (the two really difficult questions simply assumed away), then would such a regime be constitutional?

The place to start in answering this question is a recent Supreme Court case touching on the right of anonymity, *McIntyre v. Ohio Elections Commission*.[36] Ohio had a statute that made it illegal to distribute unsigned brochures relating to an election or ballot issue. The state defended the statute on the ground that it would reduce fraud or misleading statements at the time of an election. The Supreme Court, in an opinion by Justice Stevens, struck down the statute. A clear practice, both at the founding, and in the two centuries since, made it plain that speech did not lose its First Amendment protection simply by being anonymous; this speech in particular (political speech) did not lose its First Amendment protection by being anonymous; thus, because the statute burdened political speech, the Court applied "exacting scrutiny," upholding the restriction "only if it is narrowly tailored to serve an overriding state interest."[37] Because this regulation reached anonymous speech generally, the Court held, it reached too broadly.

McIntyre establishes a constitutional principle of anonymity, though no doubt a limited one.[38] It is a rule that is consistent with the original practice: While the framing world was not an anonymous one, it was clear that one had the right to build walls. One could take steps to make one's stuff private, by putting it behind walls. As a balance to constant publicity, one could take steps to keep one's identity secret, and these efforts at concealment were respected.

McIntyre, however, leaves open the question whether this right to build walls is absolute. Or, more generally, whether the government can regulate the kinds of walls one builds. One might look to the Framers' practice to resolve this question, hoping for a clear answer there. But the short and inescapable conclusion of such a search is this: that there is no original practice there to find. Government didn't regulate the kind of anonymity one was allowed, in part because there was no way to regulate the kind of anonymity one was allowed. Technology didn't allow it, and anyway, the kind of anonymity one could achieve was easily enough broken without

---

36 115 S. Ct. 1511 (1995).

37 *Id.* at 1519.

38 The Court was explicit that the opinion reached "only written communications and, particularly, leaflets of the kind Mrs. McIntyre distributed." *Id.* at 1515 n.3.

such regulation. If we are to look to the Framers for guidance, what is required is not obedience to what they thought, but elaboration from what they did.

One elaboration might be this. While we know that intentionally created anonymity was not anathema to the framing generation, we also know that even the thickest walls had to yield to a court order to open. When sufficient cause existed to demand the right to search, the power to search was upheld. The constitutional question about anonymity then comes to this: Whether the government has the right to regulate anonymity, so as to assure the ability to search when it has the right to search.

Consider a regime like this.[39] On every transaction in cyberspace, automatically there would be attached an encrypted fingerprint.[40] This fingerprint would be meaningless to anyone save one who held a key; but to one who held the key, the identity of the sender, and perhaps its content, would be revealed. The requirement would be that this key must be preserved, such that the government, if armed with a warrant, would have the power to get access to it.[41]

Such a regime (assuming it worked) would preserve the benefits of anonymity. To the public, my message or identity could be hidden. And so too to the government, except when the government had judicial permission to crack this identity or content. Only then would the anonymity be broken.

What are the constitutional arguments against this regime? Others have offered extensive doctrinal and analogical analysis of this

---

[39] Again, I am ignoring the most difficult question here, namely, how one would implement this as a requirement. The technique would not be to require it by law, but to require it in the protocol of the Net.

[40] This is simply a way of tracing the transaction back to an originator, although the ability to trace would exist only if one had the key to decrypt the fingerprint. This is different from the "digital fingerprint" discussed by Data Security, Inc., a cryptography company. *See RSA's Frequently Asked Questions About Today's Cryptography* (last modified May 9, 1995) <http://ww.rsa.com/rsalabs/faq/faq_misc.html>.

[41] Note the question whether fingerprinting itself is a search has not been clearly resolved. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE 434 & n.162 (1996).

question.[42] But my sense is the matter will be resolved at a much simpler level. One might argue that the regime is too burdensome, but of course, that argument, in the present constitutional regime, would not get one far. Or one might say that requiring production of the key itself is a search,[43] but if the key were never used or produced except when a warrant existed, then it would be odd to think of this as a search. Maybe it is a seizure,[44] but then the question is whether such a seizure is reasonable and with this the essence of the problem is revealed. For my sense is that the whole Fourth Amendment question will get resolved in just this way: Given the tiny burden on any particular individual's life, and given sufficient assurance that the key would not be misused, and given the increase in privacy that any such general regime would make,[45] is there any value from the framing legal regime that would justify the conclusion that this kind of regulation could not be permitted?

I don't see such a value in our present constitutional regime. There was no legal value that preserved to the framing regime the *right* to keep stuff hidden, even in the face of a judicial warrant.[46] There may have been the *ability* to keep stuff hidden, since the technology to find it, or identify it, might have been limited. But friction doesn't convert to a right. An *argument* for this conversion is required—some reason why it makes sense. My prediction is that no

---

42 The most extensive discussion is contained in Froomkin, *supra* note 19, at 810-43; Philip R. Reitinger, *Compelled Production of Plaintext and Keys,* 1996 U. CHI. LEGAL F. (forthcoming, Fall 1996).

43 This is distinct from any Fifth Amendment question. On that, see Reitinger, *supra* note 42; Froomkin, *supra* note 19, at 833-38.

44 If it involved the taking of a physical key, of course it would be a seizure. Sodal v. Cook County, 506 U.S. 56 (1992); United States v. Jacobsen, 466 U.S. 109 (1984). Action interfering with the possessory interests of an owner would constitute a seizure as well. Arizona v. Hicks, 480 U.S. 321, 324 (1987). Taking a copy of an encryption key would be, if anything, a seizure of an intangible, which, the Court has held, over strong dissent, would be a seizure. Berger v. New York, 388 U.S. 41 (1967).

45 A encryption regime arguably would increase privacy because it would increase the marginal cost of privacy violations for both the government and the individual. *See* Lessig, *supra* note 30, at 1751 n.23.

46 However, Professor Stuntz does make a strong argument that the thrust of the Amendment's protections are substantive. *See* William Stuntz, *The Substantive Origins of Criminal Procedure,* 105 YALE L.J. 393 (1995).

such argument will be found. A fingerprint requirement in cyberspace will be held to be constitutional.

Warrant-less Search

Imagine a worm—a bit of computer code that crosses network wires and places itself on your computer—that snooped your hard disk looking for illegal copies of software.[47] The FBI, for example, might spit this critter onto the Net, and let it work its way onto disks across the country. When the worm found an illegal copy of software, it would send a message to that effect back to the FBI; if it found no such illegality, it would self-destruct. No difference in the operations of the computer would be noticed; the worm would snoop, as it were, deep underground.

This worm would be doing what the Framers would have attacked as a general search; it would be marching through hard disks across the country without any particularized suspicion. It would be searching without warrant, either judicial or factual. If all general searches were illegal, then this one certainly would be. But if it causes no disruption of the disk, at least if it discovers no illegality, and if erases itself without being discovered, then it shares few of the characteristics of a generalized search.[48] While it is a search that proceeds without warrant, it is also a search that produces no false positives. It would be like a dog-sniff at the airport,[49] though better: worms don't bite, and unless you see them, they don't terrify either.

Would it be constitutional? Odd as this might sound, my sense here again is that this inversion of the original purpose of the Fourth Amendment would be found to be constitutional. For the Fourth Amendment's test is reasonableness (one can get a warrant only with particularized suspicion, but one violates the Fourth Amendment only if one conducts an unreasonable search); and the calculation of reasonableness must look to the benefit and the harm. The benefits are clear: the criminal activity being sought would be found with little effort and with no real disruption. The primary costs would be costs to those whose criminal activity had been discov-

---

47 The example comes from Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

48 The closest analog is the dog-sniff, which the Court held "less intrusive than a typical search" since it didn't require the opening of any packages by the individual, and it was precisely targeted at contraband. United States v. Place, 462 U.S. 696, 707 (1983).

49 *Id.*

ered. These are real costs, no doubt, but they are not costs that the Fourth Amendment really reckons. The question the Fourth Amendment asks is the burden on the innocent, and here the burden is quite slight.[50]

One might think the costs extend beyond the guilty. One might think that there is an insecurity for people who generally know that they might be watched; that this worm might be crossing their disk; that they are constantly open to surveillance by the government, most of the time never knowing whether the government is watching or not.

These are, I agree, significant costs. But they seem to describe the world we live in now, as much as any world created by cyberspace. It is simply the nature of this world that most of what one does can be monitored by the police with little or no suspicion. It is not clear how, in the face of this reality of surveillance, a constitutional problem could be raised about the marginal insecurity raised by this worm. In the constitutional universe that we now have, it seems difficult to imagine the constitutional problem this worm would present.

Zoning the Net

Congress recently passed the most significant telecommunications bill since the New Deal. Within it is the Communications Decency Act of 1996 (CDA).[51] Under the terms of the CDA, it is a federal crime to send or make available to a minor (anyone under 18) any "indecent" material. Open an FTP[52] site that contains Chaucer or Balzac, send an Acrobat file with their works to a high school

---

50 *See* Louis Michael Seidman, *The Problem with Privacy's Problem*, 93 MICH. L. REV. 1079, 1088-89 (1995) (discussing the invasion with any physical search). Adler concludes "under current jurisprudence" [the imagined search] would unquestionably be `reasonable,'" Adler, *supra* note 47, at 1106, although he mounts an impressive argument to establish that such a search should not be held constitutional. *See id.* at 1109-13. *Compare* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983) (discussing a device that could perfectly identify the guilty, and concluding that its use without probable cause would be constitutional).

51 Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. For a more general discussion of the applicability of federal statutory prohibitions on obscene and indecent speech to cyberspace, see Debra D. Burke, *Cybersmut and the First Amendment: A Call for a New Obscenity Standard*, 9 HARV. J. L. & TECH. 87 (1996).

52 "FTP" stands for file transfer protocol. It is a means of sending files across the Internet.

senior, and you expose yourself to two years in a federal penitentiary.[53]

Not surprisingly, cyber-activists were enraged. Congress, they claim, would turn cyberspace into a "Disney cartoon."[54] The statute was immediately challenged; by June, two three-judge panels had struck it down—one finding it vague and overbroad, the other simply overbroad.[55] Under the statute's own terms, the case now goes to the Supreme Court on expedited review.

As the statute is written, and in particular as the cases have been litigated, this is an easier problem than it needs to have been. If the aim of the government—both Congress and the Executive—really were to remove indecency from the Net, then they blew it. Indeed, both failed so convincingly that it is hard to see the CDA as anything other than election year politics. As the case comes to the Court, one can expect it will easily affirm the judgments below. The CDA of 1996 is dead.

But there is an idea in the CDA that will not so easily die. It is the core of the CDA of 1996, and, if reenacted, could be the essence of a CDA that would pass constitutional review. This idea is, in a sense, everything that cyberspace is now becoming. It marks a revolution in what cyberspace is. The CDA is just one small part of this revolution; indeed, its least significant part.

To see the point, step back a bit from the present bill, to what should be common ground: The aim of the bill was to protect children from "indecent speech." To do this, one cannot ban all indecent material for adult and child alike. That would no doubt be effective; it would also be unconstitutional. The reason is proportionality: the First Amendment requires a more narrowly tailored approach. As the Court said in *Butler v. Michigan*,[56] to banish the adult to protect

---

53 CDA § 502 (to be codified at 47 U.S.C. 223(1)(a)) (1996).

54 *See, e.g.*, David S. Bennahum, *The Internet's Private Side*, N.Y. TIMES, Mar. 2, 1996, § 1, at 19.

55 The cases are *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), and *Shea v. Reno*, 930 F. Supp. 916 (S.D.N.Y. 1996). *ACLU v. Reno* concluded that the statute was both vague and overbroad, though there was a dissent on the vagueness ground. *Shea v. Reno* concluded that the statute was simply overbroad. Both cases were brought under the expedited appeals provisions of the statute. *See* CDA § 561.

56 352 U.S. 380 (1957).

the child would be to "burn the house to roast the pig."[57] Something more carefully focused is required.

How carefully focused depends upon the facts—upon the context within which the ban is operating, and upon the focus that is possible there. If it is extremely cheap perfectly to discriminate in who hears what, then there will be no constitutional problem with a regulation that requires perfect discrimination. The Constitution kicks in only when the technologies are not so perfect: When to comply with a legitimate objective (to protect children), one must sacrifice interests not within the objective (to make smut available to adults). In those cases, Congress's power to protect children is limited by the First Amendment rights of the adults.

Put like this, we should begin to see the link between this example and the previous two. Once again, Congress's power is contingent upon the available technologies of regulation. Some technologies facilitate efficient regulation; some inhibit it. Where a technology facilitates regulation, more regulation is permitted; where it inhibits it, less is allowed. The question then becomes to what extent Congress can take steps to require technologies that facilitate regulation. That was the question with anonymity and encryption; it is the same question raised here.

But it is raised here at a more fundamental level. Most indecency gets traded over the counter, not across the Net, or over phones.[58] Yet the greatest portion of Congress's attention has been focused on porn on the wires rather than porn on the streets. Why? Why, if most pornography exists and is consumed in real space, do legislators worry so much about porn in cyberspace?

The short answer is that porn in real space regulates itself. It regulates itself not in the sense that porn producers are responsible types, who make sure that kids don't get access to porn; rather it regulates itself in the sense that all "self-regulation" is regulation—through social structures and social norms, some actively constructed, others evolutionary, that channel porn in real space to a particular place in real space, and discriminate with some effectiveness in its distribution in that real space.

---

57 *Id.* at 383.

58 *See, e.g.*, Anne Wells Branscomb, *Internet Babylon? Does the Carnegie Mellon Study of Pornography on the Information Superhighway Reveal a Threat to the Stability of Society?*, 83 GEO. L.J. 1935, 1936-37 (1995). *See also* U.S. DEP'T OF JUSTICE, ATT'Y GEN.'S COMM'N ON PORNOGRAPHY, FINAL REPORT 289 (1986).

This is regulation by *zoning.* Porn in real space is regulated by keeping it in its place, and by keeping it in its place, communities facilitate the restriction in its sale and distribution. Just think about the distribution of porn in any major city: There are places where porn is sold; it is not available everywhere. These places are either designated as "adult only," or if not adult only, then sales are restricted to adults only. Sales are restricted both by rules and by norms, and these restrictions can be effective because most who would try to escape them (kids) can't easily escape identifying themselves as kids. A child, for example, enters as a child, and in the process of making or not making a sale, the seller knows that it is a child to whom he is selling.

This zoning depends upon certain features of real space—what we might call the *architecture* of real space. This architecture presents a collection of transaction costs—burdens on the free flow of porn that facilitate the control of porn. Two such costs are prominent here: The burden of geographical isolation and the difficulty of hiding who one is. These two combine to facilitate discrimination in the distribution of porn—or again, they combine to make possible the zoning of porn.

We find these features of the architecture of real space, we don't make them. We certainly have worked to change them—the burden of geography is something we have from the start struggled against; the distinctions of age have been differentially respected. But however much we have worked to modify them, for the most part, we zone given them. Regulation is subject to these features of real space, as well as facilitated by them.

By "zoning," therefore, I mean any technique used to facilitate discrimination in the access to or distribution of some good or service; and by focusing on architectures that make that zoning possible, I mean to point both to the self-conscious efforts to zone, given a particular architecture, and to the possibilities of zoning made possible by a particular architecture. The techniques and the architectures are to be understood quite broadly: The techniques refer to law, as well as social norms; the architectures include both physical features of the world and cultural histories that make regulation salient, or possible. It is zoning when a local property board by law segregates housing by race; it is zoning when the same end is achieved through contract; it is zoning when the same end is achieved through social norms; it is zoning when the same end is achieved through inertia. Each is a kind of zoning; each differs in its effectiveness; each presupposes different real world architectures.

In these terms, it takes little to see how effectively zoned real space is, not just for porn, but for all sorts of things. Real space is filled with formal and informal zonings of all sorts, controlling access to every aspect of private and public life. This access is con-

trolled on the basis of a wide range of discriminations, some perfectly valid, some suspect, some perfectly effective, some just slightly so. *In general*, you don't see homeless people wandering through Barneys; you don't see children in bars; you don't see bars in residential neighborhoods; you don't see houses next to factories. Sometimes you don't see these things because of what local governments have done; sometimes you don't see these things because of norms that individuals have internalized. In countless ways, social life is regulated by these codes of zonings; in countless ways, these codes achieve or interfere with social ends, whether enacted, or merely recognized.

I have belabored this commonplace about real-space zoning because it is central to understanding a crucial difference between real space and cyberspace, as it is now. For in the most general sense, zoning is not the architecture of cyberspace. Indeed, zoning is just what cyberspace is, or at least was, against. As it was until about two years ago, cyberspace was a place where this ideal of zoning was rejected. Here was one place where borders were not to be boundaries; access was to be open and free; people could enter and engage without revealing who they were; massive search engines would collect, in the most democratic way possible, everything that cyberspace had to offer. Its essence was captured in the irreverence of a mouse: With a click one could flash just about anywhere.[59] The very design of cyberspace was (in this period of its infancy) in contrast to the world that had constructed it: One might need a high SAT score to get into the university that provided Internet access, or one might need an ID card to enter the computer lab connected to the Web, but once beyond these real-world barriers, the discriminations stopped. Cyberspace was a place of minimal protocol and unlimited access, granted equally to anyone who was there.[60]

---

[59] The major existing search engines include AltaVista, Infoseek, Lycos, Web Crawler, and Yahoo. These services maintain indices of material on the Web. Some also index material in Usenet newsgroups. DejaNews is the most famous of these companies, but AltaVista provides the same service. With DejaNews, one can enter a subject and see all the Usenet discussions about that subject, who contributed to those discussions, and other contributions a particular author has made to Usenet. The service therefore generates a profile of speech for every contributor to Usenet. Because search engines generate different results, another company, EasyPage, allows a user to search four search engines at once, and then displays the results side by side.

[60] I am of course exaggerating the point. Even if there were no designed discriminations, there were discriminations in effect, due to different speeds of access to the Net, and differences in knowledge about how the Net functioned. Exaggerations notwithstanding, the point that follows remains valid.

It is just this feature of cyberspace that cybersmut fanatics are so concerned about.[61] For the openness of this architecture means this: That there is no "natural" or simple or "automatic" way to keep people out, because there are no natural or real borders that close off access to those who should not have access. If borders in cyberspace are not walls, if cyberspace is set against walls, if people can enter as they wish, or as who they wish, then there is no simple way to select who should go where. In the terms that I have offered, there is no architecture to zone people into their proper place. Indeed, the very idea of "people in their proper place" is anathema to c-world, however commonplace it is here. To the founders of c-world, a "proper place" is no place in cyberspace.

The architecture of cyberspace as it was, then, inhibits zoning. But it need not. The architecture could be different. If c-world is now, or just was, unzoned, there is nothing in its nature that says that it must forever remain so. Cyberspace has no permanent nature, save the nature of a place of unlimited plasticity. We don't *find* cyberspace, we build it. (If anything is socially constructed, cyberspace is.) And how we build it depends first upon the kind of place we want to make.

Thus, to say that this is how cyberspace *is* is not to say that this is how cyberspace *has to be*. And indeed, the best evidence of this is the change that cyberspace is now undergoing. Quite without governmental mandate, and indeed, without anything like a centralized process of decision, cyberspace is already becoming something quite different from what I have described. It is moving, that is, from a relatively unzoned place to a universe that is extraordinarily well zoned. The architecture of cyberspace—the software that constitutes it—is becoming quite quickly far better at facilitating discriminations in access and distribution than any equivalent technologies in real space.

The best evidence of this is the latest protocols of the Web. Browsers on the World Wide Web can (unlike earlier Internet access software) implement cgi's, or gateway technologies, that will control access based on a password; they facilitate encryption, to assure that commercial transactions can occur without fear of loss or inter-

---

[61] This is the idea motivating V-Chip technology as well, also part of the Telecommunications Act of 1996. *See supra* notes 51-55 and accompanying text. The V-Chip gives parents a way to shut out certain television programs, based on their violence rating, or other ratings to be determined. While this technology may, in a sense, reduce access to materials screened, in theory there is no reason why the technology can't also increase access. If there is a technological way to screen material, then the argument that a wider range of material should be on television becomes stronger. *See infra* notes 71-74 and accompanying text.

ference by unwanted observers; they collect profiles of places where the user has been, as a way of helping other servers "decide" what sort of customer they are serving (in principle, for example, when you access a Web server, it could see what kind of servers you have accessed in the past, and then decide which advertisement it gives you now). In these ways and many others, the Web is becoming a place where the discriminations of real space get automated in a technology of zoning. This might be good, or not—that's not my point. The point is the trend: Zoning is coming to cyberspace, with an efficiency unmatched in real space.

It is against this background that we should consider the CDA, or again, the essence of the CDA which I have suggested would survive constitutional challenge, if ever drafted and presented clearly. Against the background of an ever-increasing capacity to zone, we can understand the essence of the CDA to be this: That the government demands one more dimension of discrimination be built into the architecture of the Net.[62] As well as income, or CPU

---

62 This is the link, I suggest, between the CDA and the NII's (National Information Infrastructure) WHITE PAPER on the protection of intellectual property. *See* INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (1995) [hereinafter WHITE PAPER]. For in large part, the WHITE PAPER imagines a regime where technological protections of copyright replace legal protections. As Pamela Samuelson has argued in her contribution to this symposium and in her other writings, the most dramatic part of the WHITE PAPER's proposal is its unprecedented support for technologies that essentially privatize copyright. Pamela Samuelson, Technological Protection for Copyrighted Works [hereinafter Technical Protection], Paper presented at the Randolph W. Thrower Symposium on Legal Issues in Cyberspace, at Emory Law School (Feb. 22, 1996) (on file with author). For an excellent introduction, see Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996, at 134. These technologies will allow the person creating intellectual property fully to control who has access to this property, and on what terms. These technologies, using encryption techniques and legal prohibitions against devices that break these encryption techniques, will make it possible for providers of intellectual property to keep that property from anyone they wish, and to grant access to that property only on terms they set.

This is simply zoning applied to intellectual property. The WHITE PAPER calls on the government to push cyberspace toward a technology where the owner has complete control over its property. It wants to push cyberspace to a technology that can effectively zone out unwanted users. And just as the CDA subsidizes technologies that help screen out minors from viewing indecent material, so too the WHITE PAPER subsidizes technologies that help screen out unintended users of intellectual property from viewing that material. Both initiatives subsidize the construction of walls in cyberspace.

power, or geography, or frequency of use (all dimensions quite salient to the discriminations of the existing Net), the government has said that it wants the Net to make possible a discrimination based on age.

Now there are plenty of reasons to say why such a regulation is stupid, or unnecessary, or evil.[63] But however stupid or unnecessary or evil, something more is needed to make it unconstitutional. This something more is what I am not sure that we have. For if all this other zoning is acceptable, it is hard to see just why this addition is not.

A story might better make the point: At some point during the time when the ACLU was litigating its case against the CDA, I was asked by the ACLU to participate on a panel to discuss the regulation of cyberspace. The panel was in Chicago, and the panel discussion was hosted by Christy Heffner, president of Playboy, and a strong supporter of the ACLU. The local ACLU chapter had, on its Web site, a page describing the event, and associated with each name was a link to a Web page that might give more information about that participant. The link next to my name was the University of Chicago; the link next to Christy Heffner's was Playboy.

Just before the panel discussion, I accessed this Web page, to learn something more about the other panelists. In the process, I clicked on Christy Heffner's name. I was taken to a log-in screen, that asked me for my "I-Code." Not knowing what an I-Code was, I clicked on the button that advertised itself for the I-Code-ignorant. This took me to another screen, run by the company, I-Code,

---

63 The regulation is stupid and unnecessary because it is premature. Multiplying the technologies of zoning is the boom industry on the Net just now, and there's no reason (save politics) for the government to pass laws telling the market to do what the market is already doing. And if, in five years, amazingly, this one dimension of discrimination has not been implemented, maybe then, if the passion survives, the government should step in. It is as if the government were regulating the color of wallpaper when the world was still pouring the concrete of the foundation.

The regulation is evil if one views (as I do) this whole enterprise of zoning on the Net as something to suspect. Just at the point that we are understanding the power of this alternative world, the world is acting to turn the Web into an electronic version of this world: Working, again, to replicate, only now more efficiently, all the structures of discrimination that real world zoning achieves. To some, the beauty of the Net was just its escape from these zonings, and to those people, the CDA, just as much as cgi's, are the enemy. For a different view of its mistake, see Dominic Andreano, Comment, *Cyberspace: How Decent is the Decency Act?*, 8 ST. THOMAS L. REV. 593 (1996).

Inc.,[64] and on this screen was a form. The form asked a series of questions about who I was, how much money I made, what my sex and age were, and what my employment was.[65] Once I had answered these questions, I clicked another button, and was given an I-Code. I-Code in hand (or, rather, in my paste buffer), I was returned to the Playboy Web page. I entered the I-Code, and was immediately taken to a page where I could learn about Christy Heffner, or alternatively, about one of the most popular magazines on the Web today, *Playboy*.

This whole process took about a minute, and with this minute's investment, I am now armed with a code that will (I was promised) give me access to a wide range of Web pages that similarly limit access to the I-Code-savvy.

Why did Playboy want me to register with I-Code? What's plain is that this registration had nothing to do with the CDA—the I-Code form could not verify my age. Instead, I-Code is a system developed to provide Web sites with demographic data about who has accessed their site. Data equals knowledge, and knowledge equals money: With this demographic data, Playboy can sell advertising to its site, an extremely large source of revenue for a company like Playboy.

The I-Code system (and of course there could be any number of such systems) is not an "adult services identification" system; it could be used by any Web site that wanted to collect demographic data about its viewers, whether adult-oriented or not. In the sense I have described, however, it is a zoning device: It makes possible a kind of discrimination that before would not have been possible, by linking access to data about the would-be accessers. With this information, the Web sites can do any number of things: They could sell advertising (as Playboy no doubt does), they could in principle discriminate as to access (giving some I-Code users higher priority than others); they could in principle exclude some users. (For example, a Web site set up for women only might use an I-Code-like system to screen men from the site.)

Here then is a zoning technology, created on the Web, without the demand of a government, through the voluntary choice of Web providers, to serve and facilitate commerce in c-world by blocking access to people who refuse to give up information about them-

---

64 See the description of I-Code, Inc., at Internet Profile Corp., What's an I/Code? (visited Sept. 9, 1996) <http://icode. ipro.com/icode_descrip-tion.html>.

65 *See* Internet Profile Corp., *I/Code Registration Form* <http://icode.ipro.com/register/icode_reg _form.html>.

selves. The imbedded policy choice is this: The I-Code Web sites are available only to those who cooperate with this data collection regime.[66] It is a policy choice very different from the tradition of the Net—for again, before cgi's, and Cookies.txt,[67] access could be quite anonymous. But the question we must ask from the perspective of the CDA is whether it is a policy choice very different from the choice offered by the CDA.

Well, the obvious first point is this: That if Playboy found it to be profitable to screen access to its site using the I-Code system, why would be it be any further burden on Playboy if I-Code took one extra step to verify the age of the people to whom it gave I-Code access? If I-Code were to charge a nominal registration fee (bundled, say, with coupons to purchase five times that fee at various I-Code sites), and if I-Code were to charge for its registration fee using a credit card, then under the terms of the CDA of 1996, the I-Code would become an "adult identification number."[68] It could then be used by Playboy both for its own commercial purposes (discovering the demographics of its viewers), and the government's purpose of assuring that children don't have access to *Playboy*. If that's all it took, this would not seem to be a burden that would rise to a constitutional dimension.[69]

Again, this is not to say that it would be a good regime. Indeed, my whole point is to question a general trend, not a particular statute: The trend is this push to zoning. The CDA is just one instance

---

66 I mean cooperate in the most formal sense. Of course people could lie on the I-Code form, and one suspects that I-Code does little to verify the accuracy of the data it collects. But lying has its cost, which is internalized by the person who decides to lie.

67 Cookies.txt refers to the file kept on Netscape Web Browsers, that collects data about sites a user has accessed. This list is, under certain circumstances, available to other Web servers upon a user's entry into that Web server's domain. *See* John M. Moran, *Cybercommerce: While You Browse, Someone Else on the Web Is Taking Very Careful Aim*, L.A. TIMES, June 10, 1996, at D2.

68 CDA § 502 (to be codified at 47 U.S.C. § 223(e)(5)(B)).

69 In *Shea v. Reno*, the court considered the possibility of an I-Code-like regime, but restricted to adult services. The court acknowledged that this technology was feasible, but considered it too great a burden to require many of the sites covered by the CDA to have to associate with "adult services" numbers. 930 F. Supp. 916, 943 (S.D.N.Y. 1996). But what that argument misses, I suggest, is the facility of an I-Code-like service. For again, nothing in I-Code would demand that it be associated with adult services only.

of that trend. The *White Paper* is another.[70] Both represent not a conflict between "the Net" and the government, but a union between the government and commercial interests on the Net, against the interests of the Net as more traditionally understood. The divide is not between regulation and no regulation; the divide is between a Net where regulation as zoning is facilitated and a Net where it is not. The question this should raise is not the narrow question of smut on the Net, but the broader question of whether government has this power to domesticate the Net. The question we should be asking is not whether the First Amendment bars this one dimension of zoning; the real question should be whether cyberspace should be free of these zonings of real space.

Of course, just because private interests zone doesn't mean the government can as well. Private people restrict speech all the time in ways that the government cannot. But the link between the I-Code and the CDA does let us see the form a CDA would have to take for it to pass constitutional review. The link—as a form of zoning—points to a model of regulation that will pass constitutional review, and that the CDA can easily become.

This is the form captured by a device also described in the Telecommunications Act of 1996—the V-chip.[71] The V-chip is a technology of zoning. It is a device to facilitate automatic discrimination among the shows that come across a TV channel. (The channel switcher, of course, is a more traditional zoning technology of the same sort; its zoning, however, is less automatic.) The V-chip's method of discrimination is a coding system, that indicates what kind of show a TV show is; this coding system then allows owners to block shows that don't fit a selected profile. There is plenty of debate about the merits of the V-chip, but not much that makes a compelling argument about its being unconstitutional.[72] And indeed, I think that under existing doctrine, the V-chip is not unconstitutional.

The next CDA will be modeled on the V-chip. It will require what we might call a C-chip.[73] The C-chip, like the V-chip, will

---

70 *See supra* note 62.

71 *See* CDA § 551, and *supra* notes 51-55 and accompanying text.

72 The best here is made by Balkin. *See* J. M. Balkin, Comment, *Media Filters, the V-Chip, and the Foundations of Broadcast Regulation*, 45 DUKE L.J. 1131 (1996).

73 I don't mean a "chip" literally. In both the V-chip and CDA contexts, the relevant requirement is the software that the chips contain. In both contexts, it is

simply mandate that an Internet system be capable of certain kinds of content discrimination. The best such system would be something like the World Wide Web Consortium's PICS standard, which lets consumers select the rating system they want,[74] and then the C-chip enforces the selected rating system automatically. Sites in this C-chip c-world would be required to comply with this rating system. They would have to adopt a rating that accurately reported what kind of show (or site) it was. And while the constitutional question here will be quite complex, at least to the extent that such a system is seen as a "truth in labeling" law, I don't believe it will raise any substantial constitutional concerns.

This is not to say that such a regime *should* raise no constitutional questions—only that, under our present way of reading, it will not. For the C-chip regime will just further the process of zoning that I have already described. And while the Constitution as it is can't see much that is wrong with the zoning that there is, that does not mean that there *is* nothing wrong with zoning as it is.[75] There is lots that one might question, and whether the questions outweigh the certainties is unclear. Whether they do or not, there is a choice to be made about whether a regime should facilitate this zoning—a political choice, or collective choice, which we, collectively, have not made.

A C-chip version of the CDA will survive constitutional review; it will further this zoning of the Net; it will advance the rationalization of this space; it will make cyberspace more like real space, and in the efficiency of its technology, better than real space in its ability to discriminate. Nothing in the two three-judge panel decisions that have reviewed the CDA of 1996 should draw this conclusion into doubt. For again, for the last time, if zoning is a perfectly permissible activity in real space, what possible argument would there be that this zoning is impermissible in cyberspace? If governments have the power to define the character of real space communities, through the collection of regimes of regulation that zoning in real space is, why won't they be allowed to do the same thing in cyberspace?

---

enough that there is this (not easily removed) software, whether imbedded in a ROM chip or not.

74 See the discussion in Shea v. Reno, 930 F. Supp. 916, 945-46 (S.D.N.Y. 1996).

75 And in real space there is plenty to doubt. *See* Richard T. Ford, *The Boundaries of Race: Political Geography in Legal Analysis*, 107 HARV. L. REV. 1841 (1994); Jerry Frug, *The Geography of Community*, 48 STAN. L. REV. (forthcoming 1996).

There are plenty of arguments for this vision of a zoned cyberspace, whether for intellectual property or social interaction. There are many reasons to believe it best. But so too are there reasons to question the value of this zoning, and I'll confess, my sentiments are against the zoners. But sentiments are different from constitutional sensibilities, and these suggest that sentiments against zoning won't rise to a constitutional bar. These are battles about the best architecture of cyberspace. The zoners want to make cyberspace just like home. For good or bad, laws that make cyberspace just like home will not be found to be unconstitutional.

II. THE NATURE OF CYBERSPACE

There's a pattern to these cases that we must step back to see. At each stage, as the constraints of technology give way, or as technology makes possible a kind of control never before imagined, there is a question whether to allow these gaps to be filled with increased governmental power, or with increased protections for individual privacy. Overall, my sense is, the judicial answer will favor power, rather than privacy.

The reason is this: We haven't within our constitutional tradition principles to resist this increased pressure to, as Foucault might put it, rationalize this space.[76] The irrationality, the friction, the imperfections of real space technologies are sources of regret, not virtue. They have not been principles of virtue in constitutional thought; they have been by-products of technology, not its aim. And these by-products of friction, though constituting privacy in real space, don't generate into constitutional principle. Principle does not argue on the side of imperfection.

The point is true about cyberspace generally, but to see it more clearly, we should think a bit more about an ambiguity in what it means to speak of the "law" of cyberspace. At the start of this essay I wrote about the two kinds of constraints that might exist on the government's ability to invade one's privacy—one the constraint of law, and the other the constraint of technology. To be more accurate, we might divide the constraints of "law" into centralized norms—what we ordinarily mean by "law"—and social norms. Law and social norms are both constraints. Both are distinct from the constraints of technology: A government agent must choose whether to obey the constraints of law or social norms, but there is no choice

---

76 *Compare* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 139-40 (Alan Sheridan trans., 1977) ("to foretell, rather than tell the history, of this practice of rationalization").

about obeying the constraints of technology. The police can make a search that is unreasonable, the Fourth Amendment notwithstanding; they cannot see through walls if x-ray technology doesn't exist.

Cyberspace, too, is governed by three sorts of constraints. The first is legal constraint: laws, for example, against defamation that apply in cyberspace as well as in real space. The second is social norms: rules that have developed through a decentralized regime. They mark out real constraints in some of the cyberspaces, and they sustain themselves (mysteriously one might think[77]) in these cyberspaces: rules, for example, against advertising in Usenet, which, if violated, subject the norm violator to social sanction.[78] One chooses whether to obey both of these constraints; they are directives, but not mandates, just as a speed limit on a highway is a directive, but not physically required.

But the third constraint in cyberspace is not optional in this way. These are the rules, or laws, inscribed in the software itself—the code, we might say. Rules, for example, that require a password upon entry into a system; or that require a filename no longer than thirty characters; or that require a verified return address on a particular e-mail message; or that allow the places one's Web browser has visited to be reported to another Web browser.[79] These are constraints, just as law and social norms are constraints, but they are not constraints that one chooses to follow or not. One cannot flout the password requirement.[80] The password requirement is more like a law of nature than a law of man.

---

77 Mysteriously, given the relative anonymity and loose-knittedness of these groups. *Compare* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 177-83 (1991).

78 *See* HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING THE ELECTRONIC FRONTIER 38-65 (1993). *See also* WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN (1995).

79 Again, this is the story of the Cookies.txt file. *See supra* note 67.

80 Of course, that depends upon who "one" is. It is the cult of the hacker community to demonstrate how imperfect these perfect technologies of zoning really are. This cult has, in the main, done "the system" great service. STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 431-36 (1984). Julian Dibbell, *The Prisoner: Phiber Optik Goes Directly to Jail*, VILLAGE VOICE, Jan. 11, 1994, at 44. Some believe these hackers are the saviors of cyberspace liberty. Some believe, that is, that the presence of hackers and the technologies of encryption assure a perpetual "crypto-anarchy," (*see* May, *supra* note 18), and

Both cyberspace and real space, then, have constraints of law and social norms, and constraints of code (as in the constraints of technology). Some of these constraints are optional—people choose to follow them or not; others are not optional—people "follow" them in the sense that we follow a law of nature. In this sense at least the two worlds are the same.

But the difference is this: The constraints of code in cyberspace are written by people; they are the constraints of the software that defines or constitutes cyberspace; while the constraints of technology in real space are not the constructions of people.[81] At any one time, both constraints of technology (real and cyber) might function like a law of nature. But just as God may not plead the laws of nature as a defense, so too we, with respect to the technological constraints, or powers, of cyberspace, cannot plead "nature" as a de-

---

this anarchy will save the Net from control. This is the argument that zoning is not an increase in centralized control, but an increase in individual control.

If these optimists are right, then I am wrong, and I confess, I hope I am wrong. But I believe they are wrong because they ignore my colleague Coase, or better, they ignore the constraints of transaction costs. A tiny burden imposed by "the system" on preserving or protecting privacy will, in the end, have a dramatic effect on the extent of privacy protected. This we might call the Bovinity Corollary to the Coase Theorem: Most people will simply do what at the moment seems easiest, regardless of what they think, upon reflection, of the values that "the easiest" instantiates. *See infra* note 89.

No doubt, not everyone is bovine, and especially not hackers. In presenting an argument similar to this at MIT, I was quite vigorously attacked by a hacker, who claimed I knew "nothing about" cyberspace because there was no system of security that a hacker couldn't break. My attacker revealed by his behavior that afternoon just how liberated he was from the rules that govern most: As his constant conversation during my talk revealed, he was obviously free of the most basic norms of politeness, and I don't doubt he was also free of the code of any given security system. I envy his freedom: But from the fact that "hackers could break any security system," it no more follows that security systems are irrelevant than it follows from the fact that "a locksmith can pick any lock" that locks are irrelevant. Locks, like security systems on computers, will be quite effective, even if there are norm-oblivious sorts who can break them.

81 Of course, in some sense they are. There are few constraints of technology that are absolute—the speed of light is one. But most of the rest are plastic, with some amount of effort. The intuition I am trying to develop here is the distinction between the constraints we find ourselves with and the constraints we can construct. A lock is a constraint we both find ourselves with (as we try to get into our house), and one we have constructed. But the Pacific Ocean is a constraint we find, not one we have constructed.

fense. With respect to the architecture of cyberspace, and the worlds it allows, we are God.[82]

The difference is important. Say that in the real world we wanted to stop the copyright violations of a certain book. Imagine at the start that people feel little hesitation in simply copying the book whenever they want. Society decides it would like to stop this behavior. What can it do? The most effective technique would be to issue a cop with every sale of the book, assigned to guard the book and assure it is not misused. This, however, would be a bit expensive. Alternatively, the state could institute the death penalty for copyright violations, and, if we've got the expected harm calculation correct, the fear of death might be enough to stop the violation. This, however, might be unconstitutional.[83] Or the state could do what the state does all the time, namely muck around with the social meaning of copyright theft, so that people who steal begin to be stigmatized, and this stigma begins to be internalized by people who might steal.[84] Through advertising campaigns, fines and catchy slogans, the state may slowly succeed in changing how people feel about the act of copyright theft. And if it changes this feeling enough, it may succeed in changing behavior.

What's important about this story is the slippage between the state's objective and the behavior of its citizens. This slippage is a function of the crudeness and costliness of the techniques the state has to reform or control behavior. The law can say what it will, but unless there are ways to change the incentives of individuals, what the law says will have little effect. No doubt in some communities, the fact that a law is the law is enough to change the incentives of individuals in that community (individuals, say, in that community want to be law abiders). But even then, there's a certain inertia to an individual's behavior, and even for the most virtuous citizen, a shot of changed incentives might be needed to get a change rolling.

---

82 Thus, even if one saw the distinctions here not as a distinction of kind (between constraints that we make and constraints that we find) but as a continuum, the point about cyberspace is that we have moved far toward the end represented by the constraints that we make, rather than find.

83 And as my colleague Dan Kahan argues, ineffective in any case as well. *See* Dan Kahan, *Social Influence, Social Meaning, and Deterrence*, VA. L. REV. (forthcoming Mar. 1997).

84 The WHITE PAPER, for example, recommends a campaign by the government to increase people's awareness of the problem of copyright violations, and hence to increase the extent of self-compliance, induced through stigma. *See* WHITE PAPER, *supra* note 62.

Now think about the same problem in cyberspace. Imagine that a copyright owner wants to publish a book in cyberspace, and that she doesn't want this book copied unless the reader pays for the right. What can she do? Of course, she can always rely on the same technologies of regulation that exist in real space: She can try to monitor illegal copying, she can depend upon the threats of great sanction for illegal copying, or upon the propaganda campaigns designed to induce proper behavior. But in addition to these options, the technologies of cyberspace give her something more: code. Encryption, for example, would allow the owner to encrypt her text, and release the key only to users who pay for the right.[85] Properly implemented, an encryption regime could assure that the text was properly used. It could then be a tool for assuring perfect compliance—compliance not through cooperation by individuals, but through software. Code as in software rather than code as in law would perfectly assure its own obedience.

We can summarize the point like this: While regulation in real space is primarily regulation that relies upon the cooperation of the individuals who live under the regulation, regulation in cyberspace can be something different. The code in cyberspace—the software—can enforce its control directly.

Two aspects of this difference are critical. First is the efficiency with which the proscribed behavior is controlled; second is the identity of the one doing the controlling. In the copyright example, the encryption technology both perfectly controls the behavior (by making it practically impossible to use the material without permission), and it shifts that control from public law to private. It is no longer copyright *law* that regulates how much access the public gets (through doctrines like fair use); it is instead software code. And it is no longer individuals who must choose to comply with what the law requires; the technology has made that choice for them. Copyright is privatized through the emergence of this technology of encryption, and this technology of encryption can perfectly implement the control the owner of the property wants. The technology could be different; the control could be something other than individual. But given that it is individual, it effects its result directly, without the mediation of those it would persuade.

The example from copyright suggests a more general point. Intellectual property is a public good—given that it exists, one can take

---

85 There are some complex assumptions in this statement. I am imagining a technology that would allow the user to read the text once, not to decrypt it to an ordinary text document. *See* Samuelson, Technological Protection, *supra* note 62.

as much as one wants without depleting the supply for others.[86] My illegal copy of some software, given that the software exists, will not reduce the ability of others to copy the same software. The problem, of course, is that if anyone can take the public good without paying for it, too little of the public good will be provided. The "given it exists" will not be given. To assure that the "given" is given, we must assure that a sufficiently large proportion of consumers pay for the good that they consume. This problem economists call a "collective action problem."

In real space, we solve collective action problems through what Mancur Olson calls "selective incentives."[87] A selective incentive is simply a device to assure that one pays for the public goods that one consumes. A police officer who follows you around would be a selective incentive; if you took without paying, she would punish you. But again, the cost of assigning a police officer to everyone is very high. Indeed, in general, the cost of solving collective action problems in real space is quite high. Technologies exist, but the cost of deploying them often exceeds any benefit. Hence, in a wide range of cases in real space, regulators must depend upon the threat of punishment or social meanings of stigma as the only selective incentive real space can provide. Sometimes this is enough; often it is not.[88]

In cyberspace, this could be different. There are architectures of cyberspace under which the cost of selective incentives generally could be quite low: Because one's life in cyberspace is always mediated by software, and because software can apply a selective incentive, there is an architecture of cyberspace that could more efficiently solve collective action problems. Perfectly zoned, cyberspace could be that place where there are no collective action problems—the Coasean space required by Roberto Unger's vision of plasticity; the plasticity of Unger assumed in the Coasean world.[89] Through code

---

86 On public goods and collective action problems, see DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW (1994).

87 *See* MANCUR OLSON, THE RISE AND FALL OF NATIONS 24 (1982).

88 Olson's aim is to identify the conditions under which groups can construct selective incentives, and enforce them. *Id.* at 34. But much of this analysis turns upon a relatively limited technology of control. That is the limit cyberspace will relax.

89 Ronald Coase famously described the consequences of a world where transaction costs are extremely low, as a way to direct attention to the role that transaction costs played in the construction of the market, and the firm. *See* RONALD H. COASE, THE FIRM, THE MARKET, AND THE LAW ch. 5 (1988). Roberto

as software, this architecture would implement directly the rules or incentives necessary to assure a public good's supply, by perpetually monitoring behavior in cyberspace and punishing deviance. Because one only enters cyberspace mediated by software, the code of software becomes the perfect panopticon of control.[90]

An architecture that would allow control over selective incentives that was this complete we could call, following Ackerman, "a perfect technology of justice."[91] A perfect technology of justice is one that allows policymakers to select a social end, and then assure compliance by individuals to that end. Code as software in this account becomes the means to the selected end. But for that code to function, there must be an architecture in cyberspace that supports it.

What would such an architecture be? It is not the architecture that cyberspace is just now. Right now, as I have sketched above, cyberspace is not capable of this perfect technology of justice. The thickness of the software's control, or knowledge, of behavior on the Net is quite thin. The architecture just now allows a certain resistance. People can exist on the Net anonymously; they can do things without others finding out who did what; they can encrypt their conversations without others being able to hear what they said.

But this thinness is the consequence of a choice in architectures. We could make this choice differently. It is a function of what I have called zoning. Zoning is that practice of multiplying the dimensions of discrimination possible within a system, and setting access based on those dimensions.[92] We zone when we set boundaries based on someone's age (the Computer Decency Act), on someone's willingness to pay (copyright), on someone's gender (gendered chat groups), or on someone's past purchases (advertising Web sites).

Unger described a world where it is easy to reconstruct the social structures that define social life. ROBERTO MANGABEIRA UNGER, SOCIAL THEORY: ITS SITUATION AND ITS TASK (1987). The two works are related, especially in a world of low transaction costs where social structures are constructed by definition—cyberspace.

90 For a careful, if frightening, development of this idea, see GANDY, *supra* note 20.

91 BRUCE A. ACKERMAN, SOCIAL JUSTICE IN THE LIBERAL STATE 21-32 (1980).

92 *See supra* notes 58-63 and accompanying text. In this sense, zoning is facilitated by the collection of data on individual consumption habits, what Oscar Gandy calls more generally, "the panoptic sort." *See* GANDY, *supra* note 20, at 52, 105, 108.

As we make possible this practice of zoning, we increase the facility for control.

As the number of dimensions of discrimination in cyberspace increases, we approach a world with perfect technologies of justice. At some point, when the number of dimensions along which cyberspace is zoned is sufficiently large, these dimensions of discrimination will make control possible over a very wide range of behavior. The control would never be literally perfect, but we needn't imagine the Net changing much to be able to imagine it controlling much more than it controls now.

Zoning, then, increases the potential for control. But because the structures of this control are varied—whether at the individual or collective level, whether public or private—there is plainly a range of architectures that could manifest this increase in control and a choice to be made among these architectures. The choice will manifest a perpetual tension between the relatively open and relatively closed architectures that the Net could become. The push will be strongest, I suggest, toward a world where efficient regulation is possible, and away from a world where friction makes regulation and plasticity costly. But that is just a push; it is not a necessity. Alternatives could be imagined, and this imagination alone might be a resistance to such a push. In the best of all possible worlds, cyberspace might become a place of both architectures—where one can live in the mainstream, zoned universe, and then move into something quite different.

These are the alternatives; they are background to an ongoing constitutional debate. They leave the question, how should a court respond? If there is this struggle among these different architectures of cyberspace, what should the position of courts be in this struggle? What would constitutional fidelity mean? How would a translator in the model of Brandeis resolve the tension among these architectures of cyberspace? What would fidelity require?

Here we can return to the framework that began this essay. We come from a tradition of translation in constitutional interpretation; in a wide range of cases, the aim has been to preserve founding values as interpretive contexts have changed.[93] In the face of democratic

---

[93] For a collection of examples, see Lessig, *supra* note 13, at 1214-50. For a translation applied to the executive, see Lawrence Lessig & Cass R. Sunstein, *The President and the Administration*, 94 COLUM. L. REV. 1, 93-106 (1994). As applied to federalism, see Lawrence Lessig, *Translating Federalism*, 1996 SUP. CT. REV. 125 (1996) [hereinafter Lessig, *Translating Federalism*]. For an application to the Takings Clause, see William Michael Treanor, *The Original*

majorities to the contrary, this struggle to preserve founding values is difficult. It is particularly difficult for an institution such as the Supreme Court. This is not because the Court need fear retaliation; the Court as an institution is secure within this constitutional regime. The reason is instead the Court's own image of its proper role. In its view, its role is not to be "political";[94] its conception is that it is to be a faithful agent, simply preserving founding commitments until they have changed.

The problem, however, is that founding commitments are not easily preserved, and that sometimes "preserving" may seem to be something more. Translation, that is, may often seem to be something more. And where it may seem as if the Court is doing something more than simply preserving founding commitments, that creates the perception that the Court is acting politically.[95] It creates the impression, that is, that the Court is simply acting to ratify its own views of a proper constitutional regime, rather than enforcing the views that have been constitutionalized. Thus, one important limitation on the Court's practice of translation is that it cannot translate where the translation appears political.

But what does "political" here mean? "Political" does not refer to value choices or policy choices. Value choices or policy choices, properly ratified by the political process, are meet for judicial enforcement. "Political" instead refers to judgments not clearly ratified, and presently contested.[96] When the very foundations to a judgment are seen to be fundamentally contested, and when there is no reason to believe the framing generation took a position within this contest, then enforcing a particular outcome of translation will appear, in that context, political.[97]

Cyberspace will raise this concern most strongly. Where a framing value can be translated with some clarity or certainty, then the Court can act in a way that resists present majorities in the name

---

Understanding of the Takings Clause and the Political Process, 95 COLUM. L. REV. 782 (1995).

94 I describe this in more detail in Lessig, *Translating Federalism, supra* note 93.

95 *Compare* ROBERT H. BORK, THE ANTITRUST PARADOX 83 (1978).

96 *See, e.g.*, FELIX FRANKFURTER, THE COMMERCE CLAUSE UNDER MARSHALL, TANEY AND WAITE 82 (1937).

97 The relationship between a contested ground and a political judgment is more complex than this suggests. I discuss it more extensively in Lawrence Lessig, *Fidelity and Constraint*, FORDHAM L. REV. (forthcoming Mar. 1997).

of founding commitments. But translations in cyberspace will not always be clear. The changes in technology that raise these questions of translation implicate founding values ambiguously. The changes are not simply intrusion-enhancing—they are not simply about the power of the government to monitor more. They are also invasion-reducing: The government can monitor more, but at less cost. And it is this mix of changes that makes ambiguous just how a faithful interpretation should proceed. How the translation should proceed, when changes in both the good and the bad have occurred, will simply be unclear.

The point is not that this increased rationalization is obviously good. Indeed, in my view it is not. But regardless of one's beliefs, it is at least clear that it will be contestable whether this increased rationalization is consistent with founding principle. Arguments run in both directions.[98] And although one might believe one way is stronger, if the perception is that the meaning of the right itself is contestable, the Court's most likely response is to defer to democratic judgment.[99] If there has been one consistent constraint on the Court's willingness to translate, it has been this constraint of contestability—what I have elsewhere called, in some contexts, the Frankfurter constraint.[100] Where matters are understood to be fundamentally contested, the tendency of the Court has been to steer

---

98 This is why the problem is not just a question of which method of constitutional interpretation one adopts. One could follow a paradigm cases approach, on the model of Jed Rubenfeld, *Reading the Constitution as Spoken*, 104 YALE L.J. 1119 (1995), or a principles approach, on the model of RONALD DWORKIN, A MATTER OF PRINCIPLE (1985): In either case, the changes here would undermine a view about how best to proceed. The changes here reveal where principle has not been articulated, and where paradigm cases have not spoken.

99 In *Fidelity and Constraint*, *supra* note 97, I distinguish between the situation where the meaning of a right is contested, and where the force of a justification for overriding that right is contested. In the latter case, contestation yields greater respect for the right; in the former case, it draws the enforcement of the right into question.

100 The Frankfurter constraint exists when the grounds for a court's acting are drawn into contest. Again, when the grounds for limiting a court's action—in preserving, say, some clear constitutional right—are drawn into question, contestation has the opposite effect. *See id.* Thus, *Brown v. Board of Education*, 347 U.S. 483 (1954), for example, is not a case where the grounds for acting are contested; it is a case where the government's justifications for not acting become contested. But were the Court to establish a doctor-assisted "right to die," that would be an example of the Court acting even though the grounds for its action were contested.

clear of the contest. Not always, and not that it always should, but this has been an aspect of its practice of interpretive fidelity, and this aspect will be most prominent in the context of cyberspace.

This might seem overly pessimistic, especially when one counts the two recent cyberspace victories striking down the CDA.[101] But these opinions themselves reveal a certain instability that I fear will soon resolve itself into passivity. For throughout both opinions, the Philadelphia opinion more than the New York opinion, the courts speak as if they are "finding" facts about the nature of cyberspace. The "findings" determine the constitutional result, and both courts report their findings with a confidence that makes the world they describe seem set in stone.

These findings, for the most part, were exceptionally good. They were accurate descriptions of where cyberspace was in 1996. But they don't tell us anything about where cyberspace is going, nor about *what it could be*. The courts speak as if they are telling us about the *nature* of cyberspace, but cyberspace has no nature. Its nature is as it is designed. By striking down Congress's efforts to zone cyberspace, the two courts are not telling us what cyberspace is, but what it *should be*. They are making, not finding, the nature of cyberspace; their decisions are in part responsible for what cyberspace will become.

This fact about these findings will become more obvious as more courts consider the matter. The limits on the architecture reported in one opinion will be seen later to have been overcome in another. As these shifts occur, courts will, more and more, feel that they can't really say much about what cyberspace is. They will see that their findings affect what they find.

This is Heisenberg applied to constitutional law. It is a phenomenon that is quite common. My sense is that it will yield here as it has yielded in other areas. It will yield deference: If these judgments are policy, they will be left to policymakers, and policymakers are people other than judges.[102]

That is skepticism fed by high theory. A more prosaic ground might be this: If constitutional protection for privacy is the guide, then when one reviews the history of the Court's protections of privacy since *Katz v. United States*,[103] it is hard to be anything more

---

[101] Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996); ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996). *See supra* note 55 and accompanying text.

[102] I discuss this in *Fidelity and Constraint*, *supra* note 97.

[103] 389 U.S. 347 (1967).

than pessimistic.[104] The restrictions on privacy recognized since *Katz* are all restrictions far more fundamental than the ones sketched above.[105] Yet since *Katz* the Court has been quite willing to allow

---

[104] The significance of *Katz* was its rejection of property law, or "constitutionally protected places" as the determinant of Fourth Amendment protections. This allowed the Court to hold that wiretapping was a search, even though not a violation of any property right. In the place of property rights, the Court fixed on a standard articulated by Justice Harlan: that the Fourth Amendment would protect an "expectation of privacy" that "society is prepared to recognize as `reasonable.'" 389 U.S. at 361.

The problem post-*Katz*, however, is that privacy protections now depend upon this amorphous conception of reasonableness. The pre-*Katz* places had no clear post-*Katz* application, and other issues later raised had no plain application under this test either. The consequence has been the demise of Fourth Amendment protections, and the reason should not have been hard to foretell at the time of *Katz*. If Fourth Amendment protections depend upon a balance struck in a criminal case, where there is strong pressure on the courts not to exclude evidence of a crime, then, over time, one should not be surprised to find an ever-decreasing scope of constitutionally protected domains. The virtue of the property rules was that an independent body of law defined their scope or buttressed the support that the Fourth Amendment gave. But once cut loose from this, the domain of privacy has been eroded. See Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1752 n.2 (1994), for a discussion of the post-*Katz* criticisms. *See also* DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 65-66 (1979).

The Hon. Stanley F. Birch of the Eleventh Circuit Court of Appeals, respondent for my paper at the Thrower Symposium, was more optimistic than I. I confess I hope he is right. He himself has very strong credentials as a judicial translator. His decision in *CNN v. Video Monitoring Services of America, Inc.*, 940 F.2d 1471 (11th Cir.), *vacated*, 949 F.2d 378 (11th Cir. 1991), *appeal dismissed*, 959 F.2d 188 (11th Cir. 1992), evinces an admirable sensitivity to the influence of technology on fundamental freedoms. That case involved the collision of copyright law and the First Amendment interests, and the opinion is careful to protect First Amendment interests in light of the changing technologies of publication. Were the trend in the Fourth Amendment cases the same, I would embrace Judge Birch's optimism. But I haven't yet seen this trend, from judges in general, or this judge in particular. *See* United States v. Robinson, 62 F.3d 1325 (11th Cir. 1995), *cert. denied*, 116 S. Ct. 1848 (1996) (Fourth Amendment held not to protect home owner against infrared thermal detection device).

[105] The list of cases denying a right to privacy is long, no doubt some quite reasonable, but the collection compelling in the trend it suggests: California v. Greenwood, 486 U.S. 35 (1988) (garbage left for collection); Griffin v. Wiscon-

this reduction in the protections of privacy. Its willingness there does not promise much protection in cyberspace. The practice of a codifying regime, even enhanced with the tools of translation, will not function well when the foundations of that regime change so fundamentally.

CONCLUSION

The Framers armed us with a certain set of protections, legal protections, that would preserve a certain domain of liberty against arbitrary governmental invasion or oppression. For more than two hundred years, we have been tapping this constitutional past for the answers to constitutional problems of the present. We have engaged in a practice that I have called translation to carry their values forward to our time. For the most part, this has been a relatively successful enterprise. The world has changed, technologies have changed, but the changes have been along a continuum; within these bounds, the proper judicial response was relatively clear.

I have argued in this essay that the well is about to run dry. While constitutional law has responded somewhat to the gaps created by the changes in these technological constraints, cyberspace is about to deliver a shock to this practice unlike any that it has con-

---

sin, 483 U.S. 868 (1987) (warrantless search of probationers' homes); O'Connor v. Ortega, 480 U.S. 790 (1987) (government employee's desk); United States v. Dunn, 480 U.S. 294 (1987) (barn); Dow Chemical Co. v. United States, 476 U.S. 227 (1986) (aerial photographs); California v. Ciraolo, 476 U.S. 207 (1986) (flyovers); New York v. Class, 475 U.S. 106 (1986) (vehicle identification numbers); Maryland v. Macon, 472 U.S. 463 (1985) (list of magazines offered for sale); California v. Carney, 471 U.S. 386 (1985) (automobiles, even if "automobile" is a mobile home); New Jersey v. T.L.O., 469 U.S. 325 (1985) (public school searches); Oliver v. United States, 466 U.S. 170 (1984) (open fields); United States v. Knotts, 460 U.S. 276 (1983) (movement of automobile, even if data collected by an electronic device attached to the car); United States v. Ross, 456 U.S. 798 (1982) ("automobile exception" means lesser expectation of privacy); Smith v. Maryland, 442 U.S. 735 (1979) (devices for recording the telephone numbers dialed); United States v. Miller, 425 U.S. 435 (1976) (bank records); Cardwell v. Lewis, 417 U.S. 583 (1974) (paint on car); United States v. Dionisio, 410 U.S. 1 (1973) (sound of one's voice).

The general weakness of the Fourth Amendment's protections of what Susan Freiwald calls "communication attributes" is well presented in Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996).

fronted before. The changes that cyberspace will make will bring about a process of rationalization unlike any seen before.

What then is a court to do? Commentators have offered two sorts of counsel. One has been the counsel of restraint. This new space, academics such as Cass Sunstein have argued, presents so many questions that we can't yet fathom.[106] It would be best, therefore, for courts to be extremely deferential to the actions of democrats here. Deference means standing out of the way, and letting ordinary practice and understandings catch up to the technology.

The second has been the counsel of activism: This new space, the activists have argued, requires a very active judicial response, to protect individual rights against increasing governmental and private rationalization. This is the counsel of the new ACLUs in cyberspace[107]—EFF,[108] or CDT,[109] or Barlow[110]—libertarians in cyberspace who want the government kept out.

However attractive this ideal of activism is, I am skeptical that courts will pursue it just yet, and I am not sure I would want them to. I'm not sure I would have wanted the courts to resolve the question of privacy on telephones four years after telephones became commonly used; I feel the same about cyberspace.[111] Courts can pursue actions against democrats when there is clear authority, in either text or tradition, for pressing against democrats. But there is no such tradition yet with respect to essential questions that cyber-

---

106 Cass Sunstein, *In Cyberspace, Constitutional Lawyers Should Be Quiet*, 1996 U. CHI. L. FORUM (forthcoming Fall 1996).

107 The old ACLU is in cyberspace as well. *See* <http://www.aclu.org> (visited Sept. 9, 1996).

108 *See* The Electronic Frontier Foundation (visited Sept. 9, 1996) <http://www.eff.org>.

109 *See* Center for Democracy and Technology (visited Sept. 9, 1996) <http://www.cdt.org>.

110 *See* ACLU, *ACLU Freedom Network* (visited Sept. 9, 1996) <http://www.eff.org/~barlow>.

111 Thus, certainly the worst feature in the CDA is the provision providing for accelerated judicial review. Within a year, § 561 requires the matter be ruled upon by the Supreme Court. In my view, this is too soon. If there is any context in which the Court should let matters develop in the lower courts, it is this one. The three-judge panel deciding *ACLU v. Reno* has invested some time in learning the nature of the Net, *see* 929 F. Supp. 824, 830-49 (E.D. Pa. 1996), but there is much more that must be learned, by a much wider range of judges.

space will present. The tradition of libertarianism that the Framers may have begun took for granted structures of technology that have themselves fundamentally changed. What their tradition means in this world of change is too contested a judgment for a court just now to resolve. A court that set itself on a "CyberCLU" agenda would draw into doubt its credibility as a court, for it would exercise what would certainly appear to be something more than judicial judgment. It would draw itself into conflicts that would appear political. And this activity a court could not for long sustain.

There may be a middle way. The practice of rationalization that cyberspace will launch can be questioned; courts can force us to consider its consequences.[112] Courts can, that is, act strategically to push certain questions to the fore. When judgments are tied to fairly clear historical traditions, when limitations are compellingly similar to the original constraints, when a court can effect what plainly appears to be a mere translation, in Brandeis's sense, of a framing value into a current interpretive context—here, a court should act to limit. Courts, rather than the Supreme Court, and the more courts the better.[113] The changes we confront should force us to rethink values the Framers gave us, yet we are not yet well situated to do such rethinking. We need a diversity of views, a wide range of cases, with many judgments by many federal and state judges. It is this diversity that will generate an understanding sufficient for the courts to judge upon. And it is this diversity that will help democrats rethink what is at issue. If courts cannot give us the answer, at least they can help us reconsider the question.

This hesitation imposed by the courts should be strongest when this increase in rationalization comes from the Executive Branch, rather than the legislature. For reasons outlined by Charles Black long ago,[114] where the push for increased rationalization comes just from the executive, one cannot assume it reflects a considered political judgment by the people's representatives. Here in particular is a need for the courts to question. If government is to move to further

---

[112] This has long been the argument of Guido Calabresi, directed towards the Court's practice of judicial review generally. *See, e.g.*, Guido Calabresi, *The Supreme Court, 1990 Term: Foreword: Anti-Discrimination and Constitutional Accountability (What the Bork-Brennan Debate Ignores)*, 105 HARV. L. REV. 80 (1991).

[113] Lessig, *supra* note 30, at 1754.

[114] CHARLES BLACK, STRUCTURE AND RELATIONSHIP IN CONSTITUTIONAL LAW 73-88 (reprint ed., 1983).

undermine the domains of privacy, then at least it should do so with the blessing of the most democratic branch.

Whether this third way is possible or not, a more fundamental (perhaps darker) point remains. The Framers gave us a Constitution for one kind of world; that was a world where technology was imperfect. In that world, liberty ruled, but it ruled not so much because positive law created it; it ruled more fundamentally because imperfect technologies of justice yielded to it.

When the technologies of that world change, we confront a choice. We could imagine allowing efficiency to rule this new space, by allowing liberties protected by imperfection to fall away; or we could imagine recreating spheres of liberty to replace those created by imperfections in technology. These are our democratic choices, and real choices they are.

Our problem is that our Court will not choose between the two. My sense is that the Court will simply follow the government's push to the first. It will follow the first in cyberspace, because in the main, it has followed the first in real space as well. It has allowed efficiency to flourish—for who could oppose efficiency? There is neither a well-established tradition to interfere with this efficiency in real space, nor a well-established principle for showing why cyberspace should be different. We are, at the moment, marching down a path that will yield a cyberspace very much like real space—zoned and rationalized—and we are so marching because we don't have well-developed alternative structures for directing our march any differently.

We haven't, that is, well-developed democratic structures. We need to resolve what our values will be. Yet we haven't much of a mechanism for that resolution. We want our Constitution to be codifying of values we hold to be central, and we assume that it is. But we are not in a time when we know much about what those values are, or should be.[115] There is nothing here to codify, and there is no clear vision of what we would want to transform. We are left at a stage when the Constitution can say very little to us—not because

---

[115] It is this forgetting of our own revolutionary past that motivates Bruce Ackerman, for example, in his work on American constitutionalism. *See, e.g.*, BRUCE ACKERMAN, WE THE PEOPLE: FOUNDATIONS (1991); Bruce Ackerman & Neal Katyal, *Our Unconventional Founding*, 62 U. CHI. L. REV. 475 (1995). His aim is to remind us of our constitutionally creative moments, and to teach us that the most creative are also the most recent. *See* Bruce Ackerman, *Higher Lawmaking*, *in* RESPONDING TO IMPERFECTION: THE THEORY AND PRACTICE OF CONSTITUTIONAL AMENDMENT 82, 86 (Sanford Levinson ed., 1995). But there is much here for Americans to relearn.

there are no matters of principle to resolve; there are. The Constitution has little to say to us because these matters of principle have not been resolved, and we are not well practiced in resolving them ourselves. It, the Constitution, has not resolved them, and neither have we.

Yet—we might say, if we wanted to be optimistic.