

AGAINST CYBERLAW

By Joseph H. Sommer[†]

ABSTRACT

There has been tremendous attention given to the Internet over the last five years. Many groups and commentators now speak about cyberlaw as a revolution that will sweep the legal landscape. These groups also argue that new information technologies pose new and difficult problems that traditional law is unable to solve. The author first argues that cyberlaw is not a body of law in and of itself as technologies generally do not define bodies of law. Next, the author argues that it is dangerous to consider cyberlaw as its own body of law and that to do so will lead to the development of bad law. Then, the author examines whether any legal issues posed by new informatics technologies are novel. The author concludes that most legal issues posed by these technologies are not new at all and that existing law is flexible enough to deal with such issues.

TABLE OF CONTENTS

I.	INTRODUCTION	1146
II.	THE PERILS OF CYBERLAW	1150
A.	Fields of Law Are Seldom Defined Technologically	1151
1.	<i>Of Technology and Mediation</i>	1151
2.	<i>The Meanings of "Technology"</i>	1156
B.	Harms of a Technological Focus	1157
III.	NO DOCTRINAL REVOLUTION: COMMERCIAL LAW	1162
A.	The Law of Records and Messages	1163
1.	<i>Records</i>	1163
2.	<i>Messages</i>	1165
3.	<i>Is Anything New?</i>	1168
B.	Embodied-Rights Versus Account-Based Systems	1172
1.	<i>Payments</i>	1173
2.	<i>Securities Transfers</i>	1174

© 2000, Joseph H. Sommer.

† Counsel, Federal Reserve Bank of New York. joseph.sommer@ny.frb.org. I would like to thank my friends for critically caring: Denley Chew, Annette Crowley, Jane DelFavero, Karen Gifford, Stephanie Heller, Michael Schussler, Chip Sommer and Sophia Vicksman. Their friendship does not necessarily entail support for my positions; their caring creates no responsibility for my errors. The views expressed in this Article do not necessarily reflect the views of the Federal Reserve Bank of New York or any component of the Federal Reserve System.

C.	E-Contract Formation and Electronic Agents.....	1176
D.	Licensing of Software and Information.....	1185
E.	A Final Word on Electronic Commerce.....	1188
IV.	NO DOCTRINAL REVOLUTION: THE LAWS OF SOVEREIGNTY.....	1189
A.	Sovereignty, Governance, and the Internet.....	1190
1.	<i>Internet versus State: The Johnson-Post Assertion</i>	1190
2.	<i>Internet and State: The Public-Private Dichotomy</i>	1194
3.	<i>The Public-Private Distinction and Legal Doctrine</i>	1197
B.	Choice-of-Law in Banking—An Historical Romance.....	1201
C.	Jurisdiction.....	1205
1.	<i>Personal Jurisdiction</i>	1205
2.	<i>Jurisdiction to Prescribe</i>	1207
D.	Enforcement and International Cooperation.....	1209
1.	<i>Case Study: Secrecy Jurisdictions</i>	1210
2.	<i>Case Study: International Contract Formation and Public Key Infrastructure</i>	1213
V.	THE MISCELLANY.....	1215
A.	Privacy.....	1216
B.	Intellectual Property.....	1218
1.	<i>The Other Stories</i>	1218
2.	<i>Digital Rights Management</i>	1220
C.	First Amendment.....	1225
VI.	CONCLUSION.....	1227

I. INTRODUCTION

De Tocqueville always bears reading: *deja vu* all over again. Race relations? Too little has changed.¹ The lawyer's role in society? One of his most famous—and still topical—lines.² Religion? A strong force in American political life, then and now.³ America's devil-take-the-hindmost approach to income inequality? Yep.⁴ Mercifully, he missed television and the automobile. If he had figured them out, *Democracy in America* would read like this morning's newspaper, except better.

De Tocqueville is a good starting point. He is surprisingly topical: surprisingly little has changed. Is the same true for law? More specifically, is cyberlaw (or the law of the Internet) all that new, different, or distinc-

1. "When they have abolished slavery, the moderns still have to eradicate three much more intangible and tenacious prejudices: the prejudice of the master, the prejudice of race, and the prejudice of the white." ALEXIS DE TOCQUEVILLE, *DEMOCRACY IN AMERICA* 314 (George Lawrence trans., J.P. Meyer & Max Lerner eds., 1966).

2. *Id.* at 242-48.

3. *Id.* at 265-76.

4. *Id.* at 530 ("The territorial aristocracy of past ages was obliged by law, or thought itself obliged by custom, to come to the help of its servants and relieve their distress. But the industrial aristocracy of our day, when it has impoverished and brutalized the men it uses, abandons them in time of crisis to public charity to feed them.").

tive? Does it even exist? Or has Lord Mansfield, like de Tocqueville, already said most of the things worth saying?

Are these questions fair? De Tocqueville's America is not quite ours. De Tocqueville, for example, did miss the automobile and television. He also missed the cult of celebrity worship. Lord Mansfield was not the last legal innovator: consider antitrust, the administrative state, or antidiscrimination law. Technology does change, and so probably do society and law. And yet—de Tocqueville always seems current. Maybe these matters are complex.

This Article has several things to say about “cyberlaw,” or the “law of the Internet.” First, neither concept usefully exists. Very few bodies of law are defined by their characteristic technologies. Tort law is not “the law of the automobile,” even though the auto accident is the paradigmatic tort case. Nor is urban zoning “the law of the elevator.” Modern informatics technology is no exception. This argument is unaffected by the Internet's possible transformative social impact. Maybe the Internet, or other recent information technologies, will transform society, but so did the automobile. The steam engine and the Industrial Revolution probably transformed American law,⁵ but the “law of the steam engine” never existed. Why should the “law of the Internet” be any different? In other words, “cyberlaw” and “the law of the Internet” are not useful concepts.

The connections between law and technology are almost always mediated by social practice, with evidence and patent law perhaps the only exceptions. Any connections between law and technology are therefore indirect. It makes perhaps even less sense to classify fields of law by their associated technologies than it does to classify fruit by their color. At least some fruits have a unique color. But few bodies of law are associated with only one technology, and few technologies are associated with only one body of law.

Second, not only is “cyberlaw” nonexistent, it is dangerous to pretend that it exists. A lust to define the future can be very dangerous, especially when we cannot even agree on the present. A lust to define the law of the future is even worse, since law tends to evolve through an inductive accretion of experience. It is much safer to extract first principles from a mature body of law than to extract a dynamic body of law from timeless first principles. An overly technological focus can create bad taxonomy and

5. See generally MORTON J. HORWITZ, *THE TRANSFORMATION OF AMERICAN LAW 1780-1860* (1977) (describing legal changes wrought, in large part, by the Industrial Revolution).

bad legal analysis, at least. At worst, it can lock us into bad law, crystallizing someone's idea of a future that will never be.

Third, few of the *legal* issues posed by the new informatics technologies are novel. Of course, the new information technologies are novel, by definition. They may generate some novel social practices. Furthermore, novel social practices might even generate novel law. But we should not expect much novel law, for at least two reasons. First, new technologies more often facilitate existing practices than generate new ones. Second, even new social practices are often well served by traditional legal devices. Devices resembling the statute of frauds, for example, have been on the lawyer's shelf since the days of Hammurabi,⁶ ready for use when appropriate, and returned to the shelf when not.

Fourth, most legal doctrines are flexible and likely to accommodate new social practices in their interstices. Filling interstices may be a form of novelty, but can be no more than an interstitial one. Therefore, most novel law resembles an extension or amalgamation of familiar legal categories. In other words, most legal innovation is modest, and does not resemble revolution. Law is a conservative practice, drawing heavily on analogy and history. Of course, legal doctrines will change; they always do. The new information technologies will trigger some of these changes. But with a few exceptions, these changes will exist only in the details.

Fifth, substantial changes to the legal landscape sometimes occur, and they are sometimes caused by new technologies. But the process is likely to be slow. New technologies are unlikely to generate new law immediately, in part because they are unlikely to generate new practices immediately. The lags between invention, innovation, and adoption can be considerable. Add this to the conservatism of the law, and the lags can be enormous. How big? The first "cyber-statute" may have been Article 4A of the Uniform Commercial Code, promulgated in 1989, codifying the practice of bank wire transfers. Article 4A, built on no prior statute, has been very successful. Yet Article 4A was scarcely written on a blank slate. Wire transfers have existed since at least the days of the transatlantic cable,⁷ so Article 4A codified well over a century of practice.

This is not to belittle information technologies. Movable type and television are information technologies. If they were not socially transforma-

6. See *infra* note 56 and accompanying text.

7. See MILTON FRIEDMAN & ANNA JACOBSON SCHWARTZ, A MONETARY HISTORY OF THE UNITED STATES 26 & n.13 (1963). Wire transfers soon generated their own case law. *E.g.*, *Bank of British North America v. Cooper*, 137 U.S. 473 (1890); *Cutler v. Am. Exchange Nat'l Bank*, 113 N.Y. 593 (1889).

tive, nothing is. It is hard to believe that the new information technologies will not wreak major social change. But not all major social changes create major legal changes, even fewer social changes create fundamentally new fields of law, and the creation of new fields of law is a very slow process.

Finally, much of the academic commentary on cyberlaw tacitly acknowledges the points made above. Much of the best work is not really “about” cyberlaw at all. Instead, it applies existing legal doctrine or political theory to a new arena: the First Amendment and the Internet; the public-private divide and the Internet; and norm formation and the Internet. For all of these, cyberspace is just another battleground for some very old wars. We may walk away with a better understanding of the First Amendment or the public-private divide, but the main value of the Internet seems illustrative. In applying our old law to cyberspace, we see matters afresh. To risk a metaphor from another technology, the Internet can be an excellent lens for seeing other things. It is not, however, a particularly useful focal plane of legal analysis.

Part II discusses the relationship between law and technology. It makes the first two points discussed above: (1) fields of law are seldom defined by technologies because law and technology are socially mediated, and (2) attempts to define law by technologies can be dangerous.

My other major arguments—(3) there are few novel legal issues, (4) there are fewer fundamental legal changes, (5) there is a long lag between technological change and new fields of law, and (6) “cyberlaw” is a new angle on the familiar—are difficult to argue as abstract matters. It is better to take a brute-force approach. Parts III through V examine most of the fields of law tarred with the “cyberlaw” brush: commercial law, the problems of multiple sovereignty, and a potpourri of privacy, intellectual property, and the First Amendment.

Part III focuses on well-established fields of commercial law that include: electronic authentication⁸ and data integrity, embedded-rights versus account-based systems⁹ (including private currency)¹⁰ contracting with

8. *See* *Dunning & Smith v. Roberts*, 35 Barb. 463, 468 (N.Y. App. Div. 1862) (telegram authenticates sender and satisfies statute of frauds).

9. *See* 1 MALACHY POSTLETHWAYTE, *THE UNIVERSAL DICTIONARY OF TRADE AND COMMERCE TRANSLATED FROM THE FRENCH OF THE CELEBRATED MONSIEUR SAVARY WITH LARGE ADDITIONS AND IMPROVEMENTS* (1751).

10. *See* *Chapman v. Cole*, 78 Mass. (12 Gray) 141 (1858) (privately minted gold coin current in California was not money in Massachusetts).

machines,¹¹ and the licensing of information.¹² None of these fields are new; the footnotes to the previous sentence range from 1751 to 1896. We cannot expect much legal novelty in cyberspace. Perhaps the only novel topic on the list is contracting with machines that have something that resembles discretion. However, old law may suit even this novel subject.

Part IV discusses the ancient problems of sovereignty in law. Some recent scholarship asserts that new communications technologies have transformed this old problem. Part IV discusses some of the favorite topics of this literature: the Internet and sovereignty, the public-private divide, and the three subfields of the conflict of laws: choice-of-law, jurisdiction, and enforcement. Again, there is little novelty in this domain.

Part V briefly discusses three issues common in the cyberlaw literature: privacy, intellectual property, and the First Amendment. For privacy, it argues that recent information technologies, such as the Internet or personal computer, are relatively insignificant compared to more established information technologies, and do not deserve the attention paid to them. For intellectual property, again, the Internet or other recent information technologies are not as central as one might think. One of the major trends in intellectual property is the commodification of culture, whose underlying information technologies are those golden oldies: television, movies, and recorded music. Another major trend, the business method patent, has nothing to do with technology, as traditionally understood. Quite the contrary, the business method patent seeks to expand the scope of patent law beyond technologies. Only digital rights management is a significant and novel (but not unprecedented) legal story, closely linked to current technology. Finally, much has been written about the First Amendment, and I will have little to add, but for one cautionary tale.

II. THE PERILS OF CYBERLAW

Informatics technology is socially significant, and much of it is novel. The law has already responded to this technology, and will continue to respond. What, then, is wrong with calling this legal response “cyberlaw,” or “the law of the Internet,” or something similar?¹³

11. A nineteenth-century court adverted to “ancient vessels, from which holy water would be released by a coin put through a slot.” *Am. Automaton Weighing Mach. Co. v. Blauvelt*, 50 F. 213, 214 (E.D.N.Y. 1892) (addressing vending machine technology).

12. *See Exch. Telegraph Co. v. Gregory*, 1896 Q.B. 147 (property rights exist in stock quotes).

13. This Article uses the terms “cyberlaw” and “law of the Internet” interchangeably. This cavalier attitude is only defensible because both categories are nonexistent (or

The answer is twofold. First, a technological label does not stick to most fields of law. Legal categories do not break naturally on technological fault lines. Although "cyberlaw" is a possible category, it is not a particularly appropriate one. Just as librarians do not classify books by their associated color, lawyers should not classify fields of law by their associated technologies. We may vaguely remember that Abraham Lincoln was a "railroad lawyer," but we have long forgotten about railroad law. More recently, we have forgotten "the law of space," or "the law of nuclear power." Perhaps we will forget cyberlaw once the Internet is no longer the technology *du jour*. Our law will still govern railroads, power plants, and even the Internet. But we are unlikely to associate this governing law with any particular technology.

There is a reason that these technological labels neither stick nor clarify. With a few exceptions, technology and law are mediated by social institutions, notably the market, but including others, such as government or various luminaries in the galaxy of civil society: families, religion, the workplace, communities, or the like. The law, because it regulates *social* interactions, tends to follow social dividing lines, which seldom fall along technological breaks. DNA identification, for example, may have transformed the practice of paternity testing, but has had far less effect on family law than has feminism.

In addition, technological labels can be harmful. They can take law out of social context, both current and historical. They encourage excessive intellectual risk-taking, with very little reward. An excessively technological focus may encourage predictions of a future not likely to come about. Such predictions might be hastily enacted in law, but may be far more difficult to rescind.

A. Fields of Law Are Seldom Defined Technologically

1. *Of Technology and Mediation*

To demonstrate that it is usually useless to define a body of law in terms of a technology, we begin with a fable—mostly true.

In 1793, while the "peculiar institution" of slavery was quietly dying of its own economic inefficiency, Eli Whitney invented the cotton gin. Cotton became King, and slavery became profitable again.¹⁴ Law, com-

so I argue). However, if these categories did exist, cyberlaw would encompass the law of the Internet. The latter term would probably be reserved for issues such as the domain name system, web-linking, and the like.

14. See PETER KOLCHIN, *AMERICAN SLAVERY 1619-1877*, at 94-95 (1993). It is only fair to say that Kolchin also credits steam, which powered new British spinning and

merce, and society rapidly adapted to the new profitability of slavery. This new technology profoundly influenced antebellum commercial law,¹⁵ human rights law,¹⁶ family law,¹⁷ and potentially the law of electronic commerce.¹⁸ In the years 1865-67, the law of the cotton gin reached as far as the U.S. Constitution, with the adoption of the Thirteenth through Fifteenth Amendments. In the latter decades of the nineteenth century, the older law of the cotton gin began to re-emerge, with the advent of Jim Crow.¹⁹ This retrograde trend, in turn, was checked in the early twentieth century²⁰ and has subsequently retreated.

Enough already: it's a silly fable. The law of race relations is not the "law of the cotton gin." True, the cotton gin transformed the economics of slavery, profoundly changing U.S. history and law. The cotton gin was therefore *necessary* for our subsequent legal experience with race. But then again, so was the boll weevil. "Necessary" does not imply "relevant" or even "particularly interesting."

On the other hand, oil and gas law is not at all fabulous, and teaches something else about the relationship between law and technology. Although the extraction of oil and gas is largely a matter of technology, oil and gas law does not regulate this technology. Rather, it is a real property law, which defines rights to fluid subsurface mineral deposits. Oil and gas law is a distinctive property law because of a physical fact and a social usage, not any technology. Ordinary real property law—a social construct—is usually defined by the surface property line. Mineral rights are usually defined by the cone delimited by the surface property line and converging at the center of the earth. But fluid subsurface minerals, when extracted at the surface, respect neither the line nor the cone. Their seepage across the cone creates a boundary externality. Property law has a hard time dealing with boundary externalities, and usually relegates it to the ancillary laws of nuisance and easements. But boundary externalities

weaving technologies, for increasing the demand for cotton. My story would be the same with either technology.

15. See Ariela Gross, *Pandora's Box: Slave Character on Trial in the Antebellum Deep South*, 7 YALE J.L. & HUMAN. 267 (1995).

16. *E.g.*, *The Amistad*, 40 U.S. (15 Pet.) 518 (1841); ROBERT COVER, *JUSTICE ACCUSED* (1975).

17. See Eva Saks, *Representing Miscegenation Law*, 8 RARITAN, Fall 1988, at 39.

18. See *infra* text accompanying note 119.

19. See, *e.g.*, *The Slaughter-House Cases*, 83 U.S. (16 Wall.) 36 (1873); *Plessy v. Ferguson*, 163 U.S. 537 (1896); C. VANN WOODWARD, *THE STRANGE CAREER OF JIM CROW* (1955).

20. See, *e.g.*, *Bailey v. Alabama*, 219 U.S. 219 (1911); *Clyatt v. United States*, 197 U.S. 207 (1905).

dominate the surface extraction of fluid subsurface minerals, thus requiring a different kind of real property law.

So oil and gas law has little to do with any kind of technology. Instead, it is driven by a nontechnological social practice constrained by physical fact. Change the social practice and the constraining fact becomes insignificant. Oil and gas law would merge into ordinary property law if estates were large enough. With sufficiently large estates, a typical extractable subsurface fluid mineral deposit would be far larger than cross-border seepage, and we could relegate the seepage problem to nuisance or easements. But most estates are smaller than subsurface mineral pools so oil and gas law is necessary.

Oil and gas law teach us that a constraining natural fact does not make a “law and technology” or a “law of technology.” Eyewitness evidence is not the “law of optics” because the human eye requires light. The law of personal injury is not “the law of lesions” because the human body is frail and subject to pain. Technology is not a natural fact. It is a social endeavor, albeit one constrained by natural or logical sciences.²¹

Cyberlaw is certainly not like the law of gas and oil, with an arguably technological label, but really a subspecies of very familiar law constrained—like anything else—by natural facts. Is cyberlaw fabulous, like the law of the cotton gin and automobile? Or is it completely nonexistent? This may be a Hobson’s choice, but there is likely no third alternative. With the exceptions of patent law and parts of the law of evidence, useful bodies of law will seldom be defined by technologies.²²

21. Kuhn has told us that the process of even natural science is also a social endeavor, but its product might not be. THOMAS S. KUHN, *THE STRUCTURE OF SCIENTIFIC REVOLUTIONS* (2d ed. 1970). For purposes of this Article, I am a scientific realist and technological constructivist. Notwithstanding my reading of Kuhn on science, the product and process of technology are both certainly social. (For an attempted definition of technology, see *infra* text accompanying notes 29-31.) For example, most economists now believe that technology is endogenous to economic factors—an insight associated with Jacob Schmookler. See Jacob Schmookler, *Technological Change and the Law of Industrial Growth*, in *PATENTS, INVENTIONS, AND ECONOMIC CHANGE* 70 (Zvi Griliches & Leonid Hurwicz eds., 1972).

22. Patent law, unlike almost any other body of law, must directly respond to the scientific epistemology of technology. For example, the utility requirement of patentability is usually trivial, requiring only that an invention be useful for a legal purpose. However, the utility requirement is key to chemical patents. Old chemicals can receive new patents for newly discovered uses. The law treats chemical patents differently because it is very difficult to infer useful functions of a chemical from its structure. The law of evidence, to some extent, directly reacts to the technological frontier, without much social mediation; consider DNA testing, for example. Furthermore, patent law directly constructs the social category of “technology,” through patentable subject-matter require-

Like technology, law is also a social endeavor, albeit a very different one than technology. To be sure, technology affects society, often profoundly. And so does law. And society, in turn, affects both technology and law. But the links between law and technology are seldom direct. Law and technology are usually mediated by other social forces, notably, but not exclusively, the market.²³ The cotton gin is a marvelous example: a new technology with a profound causal impact on law. Yet, its impact was socially mediated and contingent on many factors—slavery, foreign and Northern textile industries, fashion, capital flows, steam power and transportation networks, metallurgy, chemistry, Christianity, the intellectual and political ascendance of free trade, and so forth. To call the resultant legal regime “the law of the cotton gin” sounds very thin, as well as silly.

The coupling between law and technology is socially mediated. Therefore, many major technological changes may have little legal effect. For example, consider the recent revolution in manufacturing technologies: so-called “lean” or “just-in-time” manufacturing. It is difficult to think of any legal effects of this revolution, although its social effects may be large indeed. This technological revolution, for example, has been credited with smoothing the business cycle, due to lesser inventory requirements.

On the other hand, a minor technological change may have huge social or legal effects. The cotton gin, again, illustrates this point nicely. It was not Whitney’s most technologically significant invention; his interchangeable gun parts were far more important. Yet the cotton gin almost immediately transformed antebellum society, while the full impact of interchangeable parts was deferred until the latter part of the nineteenth century. As another example, indoor air cooling was a fairly straightforward adaptation of late nineteenth-century technologies. Yet it let the South rise again.

Finally—and most to our point—a major technological change may have major legal effects, without generating a characteristic body of law. A few pages back, this Article proposed the steam engine as an example.²⁴ The steam engine may have created the Industrial Revolution, and the Industrial Revolution may have been responsible for late nineteenth-century

ments. This might be less true with the advent of business method patents. *See infra* note 292. This mini-essay is hidden in the margin for a good reason. Although law and technology have some direct contacts, most contacts are socially mediated. Lawyers are concerned with greasing the wheels of commerce, vindicating individual rights, and the like. They are not technologists, except insofar as technologies shape commerce, rights, or the like.

23. *See* Schmookler, *supra* note 21.

24. *See supra* note 5 and accompanying text.

tort law, employment law, administrative law, and corporate law. But even the Gilded Age had no body of law called “steam law”; the law and the steam engine were socially mediated. Or another example: copyright. The Supreme Court has noted that:

From its beginning, the law of copyright has developed in response to significant changes in technology. Indeed, it was the invention of a new form of copying equipment—the printing press—that gave rise to the original need for copyright protection. Repeatedly, as new developments have occurred in this country, it has been the Congress that has fashioned the new rules that new technology made necessary.²⁵

Yet copyright has always been mediated through the First Amendment and the needs of the copyright industries. We do not have a “law of the printing press,” or a “law of the player piano.”²⁶

Moving closer to the present, the Internet and the telephone system use similar underlying technologies: large computers to process, transfer and store information (“servers” in the Internet; “switches” in the telephone world), fiber optics and microwaves to move information, and software galore. Improvements in these underlying technologies benefit both the Internet and the telephone system. Yet the improvements in the Internet are deemed to advance a social and legal revolution; improvements in the telephone system pass under the legal radar screen. Will the “law of the Internet” look more significant in a few years than the “law of the telephone”—a specialized body of regulatory law, of little interest outside the industry?²⁷

Even if the Internet or personal computer have the promised transformative social impact, they are unlikely to generate a characteristic body of law. Unlike other social practices, technologies seldom (directly) generate law. Although social practices incorporate various technologies, they seldom break along technological fault lines.²⁸ A new information technology is likely to affect many social practices and hence many bodies of law. However, it is not likely to generate a field of law all its own.

25. *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 430-31 (1984), *reh'g denied*, 465 U.S. 1112 (1985) (footnotes omitted).

26. *Cf. White-Smith Music Publ'g Co. v. Apollo Co.*, 209 U.S. 1 (1908).

27. See Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 568-69 (1998) (suggesting such a body of regulatory law as a category, but not exclusive category, of “Internet law”); see also Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1183 (1999).

28. An exception—industries—is discussed below.

2. *The Meanings of "Technology"*

The word "technology" has several meanings, and only one has been discussed so far: the manipulation of the physical, biological, or logical worlds to human ends. I should, however, discuss one other analytical and one other popular definition of the term. For one of these definitions, the possibility of "law of technology" may be more attractive.

We start with the alternative analytical definition of technology: the manipulation of social interactions for human ends, or perhaps even the manipulation of human desires for human ends. This broader definition is useful in many contexts, such as economics. However, the narrower definition of technology has the great virtue of separating nonsocial or non-human means (i.e., natural, biological, and logical sciences²⁹) from social or human ends.³⁰ Furthermore, the narrower definition saves us from the jarring speculation that James Madison was a greater technologist than Thomas Edison. I occasionally discuss "social technologies,"³¹ but take some care to separate these discussions from the narrower definition, which will generally prevail.

The informal alternative is much more productive. The word "technology" can refer to an *industry*, not the natural or logical techniques underlying the industry. Specifically, this word is often shorthand for part of the information technology industry, notably software, computer, and Internet firms. This informal usage has interesting implications. I have argued that technological boundaries (in the narrower sense) do not delineate social practice, and so cannot delineate law. But an industry *is* a social practice. Why can't a body of law be characteristic of an industry?

Many other fields of law also appear demarcated by industrial lines—agricultural law, aviation law, entertainment law, admiralty and—at one time—railroad law. These labels seem legitimate: they are honored by long usage, the subject of casebooks, and used unselfconsciously by practitioners. But even here, caution is indicated. Consider "entertainment law," the law appurtenant to the entertainment industry. It can be decomposed into a pastiche of employment law, intellectual property law, and tax law, among others. "Entertainment law" is not a body of legal doctrine; it is a legal practice, a very different thing. To more starkly illustrate

29. *But see supra* note 21.

30. I am not arguing that the means-ends distinction is necessarily inviolate when defining technology. *See* Laurence Tribe, *Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality*, 46 S. CAL. L. REV. 617 (1973). I assume so here merely to simplify analysis.

31. *See supra* note 22; *infra* note 292 and accompanying text (business method patents).

the difference between a body of doctrine and a practice, consider criminal law on the one hand, and criminal practice on the other. In England, they are roughly coterminous. In the United States, a defense lawyer's practice is far different than a prosecutor's, although they both deal with criminal law. Or consider the law of the horse—a viable legal practice (and industry) in Kentucky,³² but legal doctrine nowhere.

Even so, some industries—as discrete social practices—can probably support a characteristic body of legal doctrine; admiralty is a reasonably good candidate. Many bodies of regulatory law, such as banking and telecommunications, are defined by their industries. But I am not trying to construct an authoritative taxonomy of law, a probably bootless endeavor, and beyond the scope of this Article in any case. My goal is more limited. I merely maintain that no good taxonomy of law will be defined by technological boundaries, and industrial boundaries are not technological ones.

The new informatics technologies do not support any discrete body of social practice (or even legal practice), to which a characteristic body of law could adhere. These new technologies support a congeries of social practices, such as home gambling and other financial services, the practices supported by e-mail and chat lines, pornography, electronic data interchange, and nationwide garage sales. Any of these social practices might generate a characteristic body of law. But they are far too disparate to generate a collective body of law.³³ A “law of the Internet” might govern the relations between Internet service providers,³⁴ but it will not govern all legal relations affected by the Internet, because few social practices are reducible to the Internet alone.

In conclusion, the “law of” a technology is unlikely to be a useful concept, but most of the connections between law and technology are socially mediated. The “law of” an industry can be useful, but an industry is a far different social practice than a technology.

B. Harms of a Technological Focus

Even if “cyberlaw” or the “law of the Internet” has no more shelf-life than “space law,” what harm is done by a misdirected label? The literature deals with some serious legal issues: privacy, jurisdiction, commercial law, and the like. Most of these issues are old, but they are never static, and fresh analysis is always welcome. Why not re-label classical legal

32. See Miller, Griffin & Marks PSC, at <http://www.kentuckylaw.com> (last visited Nov. 26, 2000) (specializing in “commercial, corporate and equine matters”).

33. See Wu, *supra* note 27.

34. See *supra* note 27 and accompanying text.

problems as “cyberlaw” or “the law of the Internet?” What is wrong with a bit of puffery, tickling jaded palates in the marketplace of ideas?

Puffery is only harmless if nobody believes in it. Unfortunately, this is not the case for cyberlaw. This field has its true believers, who are at risk of excessive specialization and insufficient perspective, disdain for history, unnecessary futurology, and technophilia. This parade of horrors (or at least, march of disagreeables) will not infect every believer. But I believe that it has infected some, and might infect many.

The first problem—excessive specialization and insufficient perspective—shows up in several ways. An “Internet-only” focus distracts us from drawing useful connections, such as the one between traditional banking practice and modern electronic commerce,³⁵ or the Internet community and other transnational communities in civil society.³⁶ Excessive concentration on the admittedly serious jurisdictional problems posed by the Internet distracts us from the thoroughly unsatisfactory state of the modern law of personal jurisdiction.³⁷ An Internet-only focus on the law of privacy conceals the truly transformative privacy technology, the old-fashioned mainframe computer.³⁸

The second problem—disdain for history—is similar to the first problem, although it concentrates on the same legal issues as they appeared in the past, rather than cognate contemporary legal problems. A disdain for history can be lethal. Many of the legal problems of the present were seen in the past. The law—especially the common law—tends to be conservative, accretive, and inductive as opposed to revolutionary, novel, and deductive.

Part III, for example, discusses any number of legal problems associated with the law of records that have been around since the days of clay tablets. Many of the more contemporary problems (e.g., the distinction between transferable-rights and account-based systems) were well-appreciated by Lord Mansfield. Jurisdiction was a difficult problem long before the Internet, as was privacy, intellectual property, and free speech. There is nothing to be gained by an “all-Internet” perspective on these problems, or even a mostly-Internet perspective. If we pretend that these problems are recent ones, we miss a lot of relevant legal experience—several centuries, in the case of commercial law.³⁹

35. See *infra* Parts III.B, IV.A, IV.B, IV.D.2; *infra* note 275.

36. See *infra* Part IV.A.1.

37. See *infra* Part IV.C.1.

38. See *infra* Part V.A.

39. Commercial law may have the longest vitality of any modern body of law. Modern business lawyers do not hesitate to cite Mansfield, who is still the freshest word on

New information technologies are not likely to produce new fields of law, but they are likely to encourage legal analyses that incorporate, expand and generalize on what came before them. For example, Part III.A discusses a “law of records,” with antecedents in the Code of Hammurabi, that is evolving to this day. As another example, Part III.C discusses the law of “electronic agents” as an application of the law of mistake, with perhaps some antecedents in the law of slavery. The greater the emphasis on a nonexistent novelty, the less on evolution and generalization. Some of the literature already appreciates this,⁴⁰ but too much does not.

Third, futurology is a belief that we can predict future technological, social, or legal evolution. Futurology is a dangerous business, and one too prevalent in discussions of the Internet. Futurological arguments have a familial resemblance. The Internet might have a certain capacity; therefore the Internet will have the certain capacity; therefore the capacity will be used; therefore the use will have certain social effects; therefore the social effects will call for a certain legal response; therefore the lawmakers will (or should) provide such a response. Some of these arguments start later in the chain, some start earlier, but all rely on such a chain of inference. Sherlock Holmes had considerable success with these long inferential chains, but Sherlock Holmes was a fictional character. A long chain of plausible conjectures, each one dependent on a preceding conjecture, is almost guaranteed to go awry. This is even true for most natural sciences (e.g., synthetic organic chemistry), and is true *a fortiori* for social forecasting.

In the 1950s, nuclear energy was thought of as “too cheap to meter.” The marginal cost of nuclear energy was (and still is) very low; but nobody imagined the political, environmental, and other fixed costs. Also, around this time, the futurists predicted the end of checks, displaced by superior electronic payment systems. The superior electronic systems may have arrived, but checks still rule in the retail trade. They are inefficient

more than one doctrine. See, e.g., Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739 (1998) (discussing traditional negotiable instruments law in the context of digital signatures initiatives); U.C.C. § 5-105 cmt. (1999) (citing *Pillans v. Van Mierop*, 97 Eng. Rep. 1035 (K.B. 1765)); U.C.C. § 3-418 cmt. 1 (1991) (stating that the Uniform Commercial Code (“UCC”) affirms rule of *Price v. Neal*, 97 Eng. Rep. 871 (K.B. 1762)); James Steven Rogers, *Negotiability, Property, and Identity*, 12 CARDOZO L. REV. 471, 502-05 (1990) (discussing *Miller v. Race*, 97 Eng. Rep. 398 (K.B. 1758)).

40. E.g., Winn, *supra* note 39; Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Edward Rubin, *Learning from Lord Mansfield: Toward a Transferability Law for Modern Commercial Practice*, 31 IDAHO L. REV. 775 (1995).

and risky compared to these new systems, but people still prefer them.⁴¹ At the time of writing, “business-to-consumer” electronic commerce is supposed to be languishing, while “business-to-business” is supposedly flourishing. Will this still be true at the time of publication?

Internet companies make such bets on the future every day. Most of them lose, but we only hear of the successes. Futurology is the entrepreneur’s legitimate stock of trade. If they guess right, we all benefit; if they guess wrong, they face bankruptcy.

Law does not work this way. The market may reliably signal a bad business model,⁴² but there is no Chapter 7 for bad legal doctrine. Bad law stays entrenched for a while, especially when codified. There are no great social rewards for the few laws that are ahead of their times. When faced with uncertainty, the law’s response must therefore be the common law method: flexibility and a cautious fear of generalization. The premature codification of legal doctrine in response to a new technology or other social change can put a straitjacket on an as-yet-misunderstood future.⁴³

Law may contain first principles of considerable explanatory value, but these first principles are of little help in the face of novelty. For example, mature commercial law—especially payments and securities transfer law—lends itself beautifully to dogmatic exposition, probably better than any other field of law. Its expositors would certainly like to believe that their exposition is useful and real, as well as elegant. But these first principles have been much more apparent in retrospect.⁴⁴ Moreover, any An-

41. For a witty mini-essay on the perils of futurology, see Eugene Volokh, *Technology and the Future of Law in a Digital World*. By M. Ethan Katsh, 47 STAN. L. REV. 1375, 1375-77 (1995) (book review).

42. Or at least we may pretend that it does, without any harm. It makes no difference for our purposes whether bad business models die with certainty, or whether bad business models are merely more likely to die than good ones. Cf. RICHARD R. NELSON & SIDNEY G. WINTER, AN EVOLUTIONARY THEORY OF ECONOMIC CHANGE (1982). It is enough to say that bad business models die more quickly than bad legal models.

43. See Memorandum from David Bartlett, Amy Boss, & David Rice, to Uniform Computer Transaction Act Drafting Committee (May 7, 1999), <http://www.2Bguide.com/docs/50799dad.html> (last visited Sept. 19, 2000) (The Act’s “particular and detailed rules . . . sacrificed the flexibility necessary to accommodate . . . changes in technology, distribution, and contracting.”).

44. As Professor Gilmore put it for the merger doctrine of negotiable instruments law, “the courts did not start with a theory from which certain necessary consequences were deduced. Only after the courts had worked out the rules for transfer and payment was it possible to construct a theory to explain the rules.” Grant Gilmore, *Formalism and the Law of Negotiable Instruments*, 13 CREIGHTON L. REV. 441, 449 n. 15 (1979); see also Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1250-53 (1998) (explaining lack of success of

glo-American lawyer must cope with a sneaking feeling that there is no such thing as first principles, just one damned case after another.⁴⁵

There is yet another problem for legal futurology. As discussed above, law seldom operates directly on technology. It usually operates on social practices created by—or consistent with—the technology of the day. This implies a double lag between technology and law; social practice first assimilates technology, then law assimilates social practice. It is even more dangerous to predict the impact of technology on law than it is to predict the impact of technology on markets or other social practice.

Fourth, technophiles and technophobes alike ignore the complex interactions between society (including law) and technology (itself a social phenomenon, constrained by natural and logical reality). They tend to credit (or blame) individual technologies for social goods (or evils), as if the relationship between particular technologies and social phenomena were direct and unmediated by other technologies and social phenomena. At the extremes, technophiles and technophobes join a club which includes vulgar Marxists and radical libertarians: the mono-causal explanations cult. A purely technological explanation of social reality is little more useful than the opposite approach, namely holding that technology does not matter because it is merely a response to nontechnological social demands.⁴⁶

Cyberlawyers tend more toward technophilia than technophobia, although the technophobic persuasion exists among the privacy advocates. Cyberlawyers too often find the Internet as the golden thread against which the rest is mere backdrop. Everything can be explained through the Internet; the Internet changes everything.

Amended UCC Article 8, which tried to predict the direction of securities transfer law); *supra* note 7 and accompanying text (success of UCC Article 4A on wire transfers due to a century of practice before codification).

45. *But see* Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (arguing that cyberlaw is unimportant because it implicates no first principles).

46. Samuel Florman, for example, holds as “essentially true” that since engineers “did the things that society commissioned, or at least applauded, they could not be held personally responsible for any adverse consequences.” SAMUEL FLORMAN, *BLAMING TECHNOLOGY: THE IRRATIONAL SEARCH FOR SCAPEGOATS* 176 (1981). This argument suffers from at least three flaws. First, the technologist may know the adverse consequences of technology better than society. Second, technologists do not work for “society”: they work for institutions (or themselves), which may or may not be working in society’s interests. Third, respondeat superior may absolve an individual of responsibility in contract, but seldom in tort.

This kind of technophilia (or perhaps technophobia) is fine among technologists. Human rationality is limited, and deep explorations must often lack breadth and context. Narrowness is a hallmark of the specialist. Specialists maintain their *esprit de corps*, and thus their usefulness, by taking themselves more seriously than outside observers might think warranted. But, apart from some of the electronic commerce literature,⁴⁷ little in the way of “law-and-the-Internet” literature bears the earmarks of specialist expertise, narrowness, and modesty. Indeed, the “law-and-the-Internet” articles often seem to concentrate on precisely those issues in which rich social context is salient—privacy, the First Amendment, and the public-private divide. Neither technophilia nor technophobia have any place in these inquiries.

III. NO DOCTRINAL REVOLUTION: COMMERCIAL LAW

This section discusses the law of electronic commerce, which has been around since the telegraph.⁴⁸

Any discussion of electronic commerce requires a legal taxonomy, i.e., dividing “electronic commerce” into tractable categories. Any such taxonomy is largely a matter of judgment, convenience, and taste. My taste runs to the following four categories: the law of records and messages, token versus registry systems, contract formation, and licensing. These categories should cover most of the standard topics in the electronic commerce literature.⁴⁹ I could possibly have added fraud to this list, but preferred to take some specialists at their word:

The swindles over the Internet are no different from the confidence games of the past; the only difference is the medium. Thus, present antifraud weapons will more than suffice.

47. For examples, see many of the articles collected in *The Business Lawyer's* annual *Law of Cyberspace* survey. *E.g.*, 55 *BUS. LAW.* 407 (1999); 54 *BUS. LAW.* 345 (1998); 53 *BUS. LAW.* 217 (1997).

48. An opinion shared by Professor Winn. *See* Winn, *supra* note 44, at 1183. Electronic commerce may even *predate* the telegraph. Telegraphy was not the first electronic telecommunications medium—the heliograph was. (By courtesy of the Uniform Law Commissioners if not quantum physics, a photon is a species of electron. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 102(a)(27) (2000); UNIF. ELEC. TRANSACTIONS ACT § 2(5), 7A U.L.A. 20 (Supp. 2000)). Note that the technological basis for heliography dates back to Archimedes, who focused the sun on enemy ships, the better to burn them. The limiting factor was social—the human and institutional infrastructure for a network of signaling stations. This observation lies at the heart of Part II.

49. For a different taxonomy and an exhaustive treatment of topics, see BENJAMIN WRIGHT & JANE K. WINN, *THE LAW OF ELECTRONIC COMMERCE* (3d ed. 1998).

Historically, the SEC has responded quickly to evolving markets and changing industry practice, such as the foreign payments program, the municipal securities program, and the recent posture on derivatives cases. Each program shared a common theme: a commitment to protect the investor from illicit, unethical conduct within a developing legal area. Most importantly, none of the programs required any new law, rule, or regulation for successful implementation.⁵⁰

A. The Law of Records and Messages

1. Records

Most people have imperfect memories; all people die. Some people lie and cheat. There has long been a technological fix for these human frailties called “the record.” Records have legal consequences—courts generally respect them more than memory as evidence.⁵¹ But people without favorable records still want to impress courts. Some of them go so far as to fudge the record.

Record-makers do not only have to worry about record-fudgers; they must worry about snoops. The information in records is often useful to third parties, sometimes at the expense of the record-maker. Outside a commercial context, this issue amalgamates with others into something known as “privacy.” In commerce, this issue is called “data security.”

Liars, cheaters, and snoops develop snooping and record-fudging technologies to frustrate record-making and record-keeping technologies. This stimulates record-makers to invent record-security technology. This game of forgery, snooping, and security is mostly technological, and therefore highly medium-dependent. Pencil marks can be erased from paper, so ink is used instead. Customer lists may be swiped from desks, so locked vaults are used. Passwords can be guessed or otherwise obtained, so biometric aids are added to a system.

As record-makers play their cat-and-mouse game with fudgers and snoopers, the law stands by in its secondary role: neither Krazy Kat nor Ignatz, but only Offisa Pup. The lawyers’ role, although secondary to the

50. See Joseph F. Cella III & John Reed Stark, *SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium*, 52 BUS. LAW. 815, 835 (1997).

51. See FED. R. EVID. 803(6) (records “kept in the course of a regularly conducted business activity” exempt from hearsay rule); FED. R. EVID. 902 (some records self authenticating); U.C.C. §§ 3-308 (1991), 8-114 (1999) (evidentiary presumption for negotiable instruments); U.C.C. § 8-501(b) (1999) (security entitlement created by record); U.C.C. §§ 1-206, 2-201, 5-105 (1999) (statutes of frauds, demanding records for *any* legal effect).

technological war, is not trivial. The law usually (but not always)⁵² helps the record-makers and seeks to discourage the fudgers and snoopers. This section seeks to give a general account of law's role in assuring authentication, integrity, and security of data in records. In doing so, it demonstrates the continuity of "cyberlaw" with what went on before.

First, law can make detected fudging and snooping painful to the fudger or snoop, *pour l'encourager les autres*. As Lord Mansfield once so casually noted in a negotiable instruments case: "The plaintiff lies by, for a considerable time after he has paid these bills; and then found out 'that they were forged:' and the forger comes to be hanged."⁵³ As a commercial lawyer, Mansfield may have been a great innovator, but as a hanging judge, he was an enthusiastic traditionalist.⁵⁴

Second, appropriate legal rules can encourage people to use more secure records. Some rules are carrots, while others are sticks. Some sticks beat the snoop or fudger and others beat the victim. One example of the latter would be the section of UCC Article 3,⁵⁵ which places the risk of altered checks on people who write their checks in pencil. The more extreme rules of this variety punish even *potential* victim-hood. The statute of frauds, for example, penalizes those naive enough to rely on another's word without getting it in writing. This punitive device was appreciated in the Code of Hammurabi.⁵⁶ On a more sophisticated level, the law of trade secrets may offer no solace to victims who had not tried hard enough to safeguard their secrets.⁵⁷

The carrot may be as effective as the stick. Many rules reward the creation of secure records by placing them in a privileged legal position. The seal—which relied on a (hopefully) unique physical token—conferred strong advantages in the old pleading system.⁵⁸ Records kept in the ordinary course of business are more reliable than other records, and thus are exempt from evidentiary exclusion as hearsay.

52. See *infra* notes 61, 75 (surreptitious records).

53. *Price v. Neal*, 97 Eng. Rep. 871 (K.B. 1762).

54. See *Rubin*, *supra* note 40, at 781.

55. See U.C.C. § 3-406(a) (1991).

56. See Code of Hammurabi ¶¶ 122-123 (L.W. King, trans.) (bailment enforceable against bailee requires a witness or writing), <http://www.yale.edu/lawweb/avalon/hamframe.htm> (last visited Nov. 17, 2000); *id.* ¶¶ 104-105 (requiring consignee to have a receipt).

57. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40(b)(4) (1995) (recipient of trade secret through accident or mistake is entitled to use it if holder of secret had not been careful to safeguard it).

58. See J. H. BAKER, AN INTRODUCTION TO ENGLISH LEGAL HISTORY 269-71 (2d ed. 1979).

The various laws of records are well understood and this discussion has mostly sought to put them in perspective. Less familiar, perhaps, is the distinction between records and messages, and the distinctive laws of messages.

2. Messages

A message is a symbol or concatenation of symbols transmitted from a sender to a recipient. Messages are legally significant. The receipt of a message notifies the recipient as to its data content: an event that can affect subsequent rights of the recipient. The transmission of a message will often bind the sender, as with a contractual offer or a letter of credit. Occasionally, receipt of a message will even bind the recipient.⁵⁹

However, messages are not necessarily records. Records must persist to fulfill their evidentiary role. Messages associated with evanescent media, such as sound or skywriting, are legally inadequate where a record is required.⁶⁰ (However, these messages can be transformed into records through, say, tape recording or a camera.)⁶¹ Just as all messages are not records, all records are not messages. A message must be transmitted from sender to receiver, but a record need not. Private notes are records, but are not messages. There are some borderline cases. For example, a filed notice of a security interest is certainly a record. This record gives constructive notice of a security interest, even if it is unread. Is it a message, as well?

Usually messages—not records—do the legal work. Messages create the overwhelming majority of legal relations, especially contractual ones. Some contracts—particularly unilateral ones formed by performance—are not formed by messages, but these are in the minority. The messages that form contracts are not necessarily records. Oral contracts are often fine. For our purposes here, records usually have a modest function—they merely evidence messages.⁶²

59. See U.C.C. §§ 4A-209(b)(3), 404(a) (1989).

60. *E.g.*, *Reed v. Woodward*, 11 Philadelphia Reports 541 (Ct. Common Pleas 1875) (chalk on slate did not qualify for will).

61. This point may not be as obvious as it seems. Courts have contested the evidentiary value of both tapes and photographs. *Compare* *Ellis Canning Co. v. Bernstein*, 348 F. Supp. 1212 (D. Colo. 1972) (tape recording a record for statute of frauds purposes), *with* *Sonders v. Roosevelt*, 476 N.Y.S.2d 331 (App. Div. 1984) (surreptitiously-obtained tape not a record). See also Jennifer M. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J.L. & HUMAN. 1 (1998) (recounting acceptance of photography as evidence in nineteenth century).

62. Records have an independent significance in intellectual property law. See *infra* text accompanying note 325. Records also have a separate role in negotiable instruments and their electronic equivalent. See *infra* notes 83-87 and accompanying text.

Much of the law of messages is substantive. Which symbols, under which circumstances, have which legal consequences? This substantive law—a matter of the significance of the message's data content—is embedded in other bodies of law and is not of concern to us. But few messages are as transparent as their data content. Technologies or agents mediate most messages. Perhaps a handshake agreement is unmediated, but a telephone call is heavily mediated: machines at both ends, machines and wires in the middle, and telephone numbers serving as identifiers. The adjective law of messages is this law of mediated messages.

Any law of mediated messages must solve several issues, none of them self-evident from the physical or data structure of the message. *Is the message authentic?* If the message was transmitted over a secure system, do we care about any other evidence of authenticity?⁶³ *When was the message transmitted?* When placed in the mailbox? When the user hits the "transmit" key? At the time evidenced by a third-party date-stamp? *When was it received?* When it creates actual notice? When the post office or recipient's ISP delivers it? *By whom was it transmitted or received?* This is necessary to resolve issues of authority, intermediary liability, and organizational notice. *Is the message in an appropriate format?* Proper language? Proper encryption? Are the right symbols in the right fields? Proper medium?

Traditionally, the answers to these questions have been left to the common law, supplemented by statutes such as the UCC. The Uniform Electronic Transactions Act ("UETA") provides a statutory answer to many of these questions for electronic messages,⁶⁴ although even it has not tried to solve all of these issues. Many of these answers track the common law closely, while others are novel. But these questions have been around for a long time.

In our bureaucratic society, we sometimes lose sight of the primacy of messages, and the mere evidentiary function of records. For example, lawyers often loosely refer to a bank's "books and records" as creating

63. Several e-commerce statutes state that transmission over a secure system creates a presumption of authenticity: so-called "hard authentication." *E.g.*, U.C.C. § 4A-202(b) (1989); UNIF. COMPUTER INFO. TRANSACTIONS ACT § 108 (2000); UNCITRAL Model Law on Electronic Commerce (MLEC), art. 13, 36 I.L.M. 197 (1997). In contrast, UETA demands that the party who benefits from an authentication must prove it from the facts of the case. *See* UNIF. ELEC. TRANSACTIONS ACT § 9, 7A U.L.A. 32 (Supp. 2000).

64. *See e.g.*, UNIF. ELEC. TRANSACTIONS ACT § 10, 7A U.L.A. 33 (Supp. 2000); *id.* § 15, 7A U.L.A. 38-39.

legal rights, a habit carried into some statutes and regulations.⁶⁵ However, case law clearly shows that bank records are not necessary to create an entitlement against the bank if some other adequate evidence of the appropriate communication exists.⁶⁶ Currently Article 1 of the UCC seems to note the distinction between records and messages, with “telegram” doing the work of “message” (more specifically, “electronic message”) and “writing” doing the work of record.⁶⁷ However, “telegram” was not much used in the old UCC,⁶⁸ and has been dropped from the current draft of revised Article 1.⁶⁹ The new wave of electronic commerce friendly statutes has a useful and general definition of “record,”⁷⁰ but has no cognate definition of message. UCC Article 4A—a pure law of messages—does not use the word “message” in the statutory text.⁷¹ UETA—although calling itself a law of records and signatures—is largely a law of messages.⁷² The law of messages is a familiar—if tacit—part of the old UCC. For example, the UCC has an elaborate treatment of the legal problems of messages received by organizations, under the rubric of “notice.”⁷³ Only the Model Law on Electronic Commerce (“MLEC”) seems to draw a reasonably

65. *E.g.*, U.C.C. § 8-501(b)(1) (1999) (“book entry”); 31 C.F.R. § 357.21(b) (2000) (“marked on the books”).

66. Take the wonderfully named case of *FDIC v. Records*, 34 F. Supp. 600 (W.D. Mo. 1940), or *Singer v. Yokohama Specie Bank*, 58 N.E.2d 726, 728 (N.Y. 1944), or cases cited in Joseph H. Sommer, *Where is a Bank Account?*, 57 MD. L. REV. 1, 23 n.60 (1998). The so-called “*D’Oench, Duhme* doctrine” codified in 12 U.S.C. § 1823(e) is an exception: real records are certainly required. 12 U.S.C. § 1823(e) (1994). However, this doctrine is a creature of regulatory law, not commercial law.

67. Compare U.C.C. § 1-201(41)(1999) (“‘Telegram’ includes a message transmitted by radio, teletype, cable, any mechanical method of transmission, or the like.”), with U.C.C. § 1-201(46) (1999) (“‘Written’ or ‘writing’ includes printing, typewriting or any other intentional reduction to tangible form.”).

68. The only usage of “telegram” in the old UCC of which I am aware is old U.C.C. § 5-104(2) (1990). And here, telegram was unambiguously used to mean “record,” as it placed electronic letters of credit within the statute of frauds.

69. See U.C.C. § R1 (2000 Annual Meeting Draft).

70. See, *e.g.*, U.C.C. § 9-102(a)(69) (2000); UNIF. ELEC. TRANSACTIONS ACT § 2(13), 7A U.L.A. 21 (Supp. 2000); UNIF. COMPUTER INFO. TRANSACTIONS ACT § 102(58) (2000) (“information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”).

71. Its key concept of “payment order” is pure message. See U.C.C. § 4A-403(a)(1) (1999) (“payment order” an “instruction”).

72. UNIF. ELEC. TRANSACTIONS ACT §§ 7-15; 7A U.L.A. 30-40 (Supp. 2000). The only sections of UETA that deal with persistent records to the exclusion of possibly-evanescent messages are 8(c), 11, 12, and 13.

73. U.C.C. § 1-201(25)-(27) (1999). Revised Article 1 has realized that the problems of notice—especially organizational notice—are problems of substantive law, not to be hidden in definitions. U.C.C. § R1-202 (2000 Annual Meeting Draft).

sharp distinction between messages and records: discussing records in chapter 2 and messages in chapter 3.⁷⁴

3. *Is Anything New?*

I have argued that there is a general law of records and messages, and that the content of this law harkens back to old legal rules. Nothing in this argument has called for fundamentally new legal principles. The idea of a “law of records and messages” might be a new organizing principle, but none of the doctrines organized by this principle are new.⁷⁵ This argument, of course, has weaknesses. It has not examined new information-processing technologies, or new media for record-retention. Arguably, new information processing or retention technologies might change the law. This subsection examines this proposition.

We start with information-processing—technological devices for assuring the authenticity, integrity, and security of records and messages. Four technologies come to mind: the trusted third party, encryption, physical tokens, and biometrics.

Records kept at and messages transmitted through a trustworthy repository are impossible to alter, easy to date and authenticate, and as public as they need to be. The only questions about such a record concern the authenticity and integrity of the record at the time of deposit. The trusted third party can mitigate this remaining problem in two ways.⁷⁶ First, parties usually have the least incentive to fudge the record at the beginning of a transaction, before the gains and losses of a deal materialize. Second, trusted third parties can be held liable for the authenticity of records deposited with them, providing them with the appropriate incentives to ensure authenticity. These liability rules are at the center of certification authority law, but easily date back to Lord Mansfield’s day. An endorsement

74. And even the MLEC does not draw this distinction in so many words, using “Application of legal requirements to data messages” as the heading for the records chapter and “Communication of data messages” for the messages chapter. UNCITRAL Model Law on Electronic Commerce, 36 I.L.M. 197 (1997).

75. A small exception might be noted. Twentieth-century technology has permitted the creation of reliable records without knowledge of the record by the party who produced the record. In other words, we now know how to tap wires and carry concealed tape recorders. (Surreptitious photographs were a nineteenth-century antecedent. See Mnookin, *supra* note 61, at 12-13.) These cryptic records may be regulated by law—sometimes criminal law forbidding the creation of such records, sometimes the statute of frauds, *see supra* note 61, and often rules of legal ethics regulating such underhanded tactics. Such laws may be genuinely novel, but are at most peripheral.

76. “Trusted third parties” has been a topic of some recent literature. *E.g.*, A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

on a negotiable instrument assures the authenticity of previous endorsements.⁷⁷ A nonrecourse endorsement has no effect *but* signature and data integrity certification, an early form of certification authority.⁷⁸ Similar is the late nineteenth-century device called a “signature guarantee,” a bank product that remains a cornerstone of paper-based securities transfer practice.⁷⁹

Physical tokens are hard-to-duplicate devices of which possession indicates authenticity of a message. Physical tokens are not only independent of specific information technologies, but they are again nothing new. The atomic spies of the 1940s could think of nothing better to guarantee identity than ripping a cardboard label in two and later matching the complementary parts together. Today’s encrypted smart card might be no more secure.

Authenticating a message by recourse to a person’s physical characteristics is both very old and very new. The manuscript signature is a very traditional biometric device. It may be easy to forge, but the thumbprint—also biometric and also traditional—is not. New biometric devices—iris scans and the like—may be technologically superior, but the idea of biometrics is old, along with the law.

Like biometrics, cryptography is nothing new, at least as far as it assures the authenticity and privacy of data. The use of cryptography in ensuring data integrity is perhaps more novel, but certainly predates the Internet. The hash algorithm has ensured commercial data integrity since at least the 1950s.⁸⁰ Look at your checks. The funny-looking machine-readable numbers on the bottom (the “MICR line”) are a fine example of

77. U.C.C. §§ 3-415 (1991), 7-507 (1999), 8-108(a) (1999).

78. A non-recourse endorser warrants that “all [upstream] signatures on the instrument are authentic and authorized; [and] . . . the instrument has not been altered.” U.C.C. § 3-415(b)(2), (3) (1999). These were the functions contemplated by the non-recourse endorsement in the old NIL era, and probably before. *See Menges v. Robinson*, 26 P.2d 882, 883 (Cal. App. 1933) (“The only reason I had him sign it [i.e., a non-recourse endorsement] was to vouch for the signatures of those men.”). A non-recourse endorsement may also serve as a quitclaim. U.C.C. § 7-505 (1999).

79. *See* EGON GUTTMAN, *MODERN SECURITIES TRANSFERS* ¶ 12.03 (3d ed. 1987).

80. The hash algorithm derives a relatively short “checksum” from an arbitrarily long string of text. The checksum is near-uniquely determined by the text, and any corruption of the text likely will produce a different checksum. By comparing a recomputed checksum with the checksum associated with the original text, one can therefore detect text corruption. *See* NAT’L INST. OF STANDARDS AND TECHNOLOGY, U.S. DEP’T OF COMMERCE, FEDERAL INFORMATION PROCESSING STANDARD PUB. NO. 180-1, *SECURE HASH STANDARD* (1995), available at <http://csrc.nist.gov/fips/fip180-1.txt>.

1950s computer technology. (“Do not bend, fold, spindle, or mutilate.”) They include a hash function.⁸¹

We now turn to media suitable for records.⁸² In most respects, record media are not unique in any particular quality. All media have some storage capacity, have some cost per symbol stored, persist for some time, have some susceptibility to physical alteration, may or may not require ancillary equipment to perceive, or the like. Electronic records are not unique in most of these qualities. True, electronically-stored data can form great searchable banks, almost uniquely. But this attribute is irrelevant to the legal problems of records: authenticity, data security, and data integrity.

Yet, electronic record media may be exceptional in one respect. In any record, the data structure is embedded in some physical medium at any given time: marks on paper or electric fields on a RAM chip. However, in traditional records, the data structure is stably associated with the medium. This is much less true for most electronic records. Most “electronic” media permit easy copying and easy erasure, e.g., magnetic domains or memory chips. As a matter of physics, a data structure remains associated with a physical structure. However, as a matter of practice, it does not. Because of easy copying, easy erasure, and complex linkages, the data structure of most electronic records is commonly identified with a *system*, not the physical *medium* in which it is embedded at any given time.⁸³ This practice is strengthened by the promiscuous way in which an electronic system replicates data structures in caches, backup memory, and the like. This is a matter of usage, not physics. We can always—in principle—find the physical medium in which the data are embedded at a given point in time. But as a matter of practice, we look to the system, not the medium. Such records are effectively independent of any medium.

If stored data are associated with the system as a whole, rather than with a physical subcomponent of the system, there is no piece of the sys-

81. See EDWARD L. RUBIN & ROBERT COOTER, *THE PAYMENT SYSTEM* 259 (2d ed. 1994).

82. Some media are not suitable for records. Instead they are suitable merely for messages. See *supra* text accompanying notes 60-61.

83. This is not necessarily true for all electronic media. Data may be permanently “burned in” to a “write-once-read-many” (“WORM”) medium. The WORM medium is subsequently specifically identifiable to the data structure. Smart cards are similar. Although eraseable, smart cards are distinct from the rest of the computer system. Therefore, data can be uniquely associated with the smart card (which is really a highly-controlled separable subsystem, rather than a distinct physical medium, as is a WORM medium). See Java Card Special Interest Group, *Smart Card Overview*, http://www.sjug.org/jcsig/others/smart_card.htm (last visited Nov. 20, 2000).

tem that meaningfully corresponds to the original record. Although all data structures must be inscribed (or embedded) in a physical medium, with most computer systems, we cannot trace a data structure from one physical medium to another. Therefore, all data structures produced by the system are equally original—because they are indistinguishable from the original. Originals and copies can only be distinguished if they are associated with physically distinguishable media. This is a very significant point. It implies that most electronic records are more limited than records inscribed in other media.

In other words, most computer systems cannot duplicate the role of an engraver: creating original media whose data structure cannot be copied without revealing that the data structure was copied. The tricks of this trade (e.g., engraving, photo-shifting inks, special papers) can frustrate even a professional forger. To make a copy conceptually indistinguishable from a well-engraved paper original, one must steal the dyes, inks, and paper. (Or—as in the famous Portuguese Bank-Note Case—one must steal currency from the printers before it has gone into circulation.)⁸⁴ However, electronic data structures, in practice, have no significant connection with the media in which they are embedded. Therefore, electronic copies are epistemologically indistinguishable from originals.⁸⁵

This quality of most electronic systems⁸⁶ is as much a curse as a blessing. An electronic “original” cannot exist in the same sense as a paper “original.” This implies that traditional paper records are more versatile, in some ways, than electronic records. They possess a property that electronic records do not. Because negotiability requires that legal rights be embedded in a transferable data structure, negotiability requires that an original be distinguished from a copy. A ten-dollar bill is money, while a photocopied bill is not. Negotiability may be on paper or the side of a cow, but it is conceptually impossible with a pure data structure.⁸⁷ Although

84. *Banco de Portugal v. Waterlow & Sons, Ltd.*, A.C. 452 (H.L. 1932). The stolen currency was counterfeit in the hands of the thief, but became good money when taken in good faith for value.

85. *Cf.* UNIF. ELEC. TRANSACTIONS ACT § 12(d), 7A U.L.A. 36 (Supp. 2000). This paragraph and the surrounding ones contain what may be an extremely informal excursus into computer science. The author disclaims any competence in the field, but requests the temporary indulgence of the reader. If indulgence is given, we see that computer science may have something to contribute to legal analysis, and perhaps vice versa. This is contrary to Judge Easterbrook’s assertion. *See* Easterbrook, *supra* note 45.

86. *But see supra* note 83.

87. *See infra* text accompanying note 89. UCC Article 9 and UETA both seek to identify the criteria for a negotiable medium. “[E]ach copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy.”

electronic records as pure data structures are therefore novel, this novelty is more a reduction of possibility than a new capacity.

Today's electronic data systems contain few new capabilities that are relevant to the laws of records and messages. Ironically, what seems to be novel is that some electronic data systems may lack a capability inherent in traditional media: the capacity to serve as the basis for negotiable instruments.

B. Embodied-Rights Versus Account-Based Systems

This subsection discusses a recent topic in electronic commerce: the distinction between "embodied-rights" and "account-based" systems.⁸⁸ Slips of paper have traditionally indicated or conveyed rights, e.g., negotiable instruments. A transfer of the paper would transfer the rights. Account-based systems—that relied on records kept in a central repository—displaced the paper thanks to the mainframe technologies of the 1950s. The shift may now be back to embodied rights systems. The Internet is arguably far more decentralized than the mainframe technology of the 1950s. The vision of electronic tokens whizzing on the Internet, conveying transferable rights, may be an attractive alternative to centralized account systems evidencing transferable rights.

This vision, although technologically coherent, poses a severe accounting problem arising from the impossibility of an original electronic data structure dissociated from any permanent medium. If trusted Server 1 says that I owe you one hundred dollars, and trusted Server 2 says the same thing, do I owe you two hundred dollars? Maybe. Or maybe the records are mere duplicates, both evidencing the same one hundred dollar debt. Or maybe I owe you nothing, because both Servers 1 and 2 reflect the same one hundred dollar debt that had already been discharged, as evidenced by trusted Server 3. This problem does not exist for centralized account systems because there is only one relevant record: the one on the unique central registry.

This accounting problem has a technological fix: a unique record. The problem is to ensure uniqueness in a decentralized electronic environment, in which perfect copies are easy to make, and originals are difficult to imagine. The problem has been solved, at least in part. One solution involves a unique physical token with authentication and record-keeping

UNIF. ELEC. TRANSACTIONS ACT § 16(c)(5), 7A U.L.A. 40 (Supp. 2000); *see also* U.C.C. § 9-105(5) (2000).

88. *See* Jane Kaufman Winn, *Electronic Chattel Paper Under Revised Article 9: Updating the Concept of Embodied Rights for Electronic Commerce*, 74 CHI.-KENT L. REV. 1055 (1999).

capacities (e.g., a smart card) associated with the electronic system. Several e-money schemes already embody such a solution.⁸⁹ But physical tokens may not be necessary. Electronic tokens that cannot be copied can be implemented on a purely electronic system—if the system contains a central registry. However, we have not seen a pure electronic token technology, aided by neither physical tokens nor central registries.

But even if pure electronic tokens cannot exist, hybrid physical-electronic or registry-electronic embodied rights systems exist today. There is no technological reason why such embodied rights systems cannot displace account systems. If the market so desires, there is no basic obstacle to abandoning accounts for embodied rights. Embodied-rights and account systems have long alternated in commercial law, as technological and social conditions favored the one, and then the other. Payment and securities lawyers are extremely familiar with this story. We will start with payments, and then go to securities transfers.

1. *Payments*

The payment side started with embodied rights: coin and perhaps bullion. These physical tokens slowly mutated into something more complex, i.e., tokens representing tokens.⁹⁰ The mutagen was the law of negotiable instruments, specifically the merger doctrine.⁹¹ This doctrine assured that physical possession of an appropriately endorsed instrument was tantamount to a claim against the issuer. The claim could be and originally was for coins. But it could be for other things as well: documents of title, securities certificates, and perhaps even other instruments.

The eighteenth-century mind viewed the business of banking as a trade in gold, the trade facilitated by negotiable tokens for gold.⁹² These circulating tokens—supplemented by coin—formed the money of the time. However, the character of money changed during the first half of the nineteenth century. People became less interested in trading coin—or tokens for coin—and more interested in trading *claims*. In other words, bank accounts become the stuff of money, rather than a representation of what had

89. For a good commercial law discussion of e-money, see The Task Force on Stored-Value Cards, *A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money*, 52 BUS. LAW. 653 (1997).

90. See J. MILNES HOLDEN, *THE HISTORY OF NEGOTIABLE INSTRUMENTS IN ENGLISH LAW* 99-143 (1955).

91. See *id.*; JAMES STEVENS ROGERS, *THE EARLY HISTORY OF THE LAW OF BILLS AND NOTES* 170-246 (1995).

92. 1 POSTLETHWAYTE, *supra* note 9, at 196.

been the true stuff—specie or perhaps banknotes.⁹³ If the claims were reliable and exchangeable enough, the entitlement underlying the claim scarcely mattered.⁹⁴ During the old gold standard days, people used bank money just as they do today, seldom converting to gold. With modern fiat money, the ultimate entitlement is completely irrelevant; only the claims on the bank count.⁹⁵

Bank accounts are account systems, not embodied-rights systems. As the economy became increasingly impersonal and trust relations increasingly institutionalized, bank account systems (which relied on the bank's integrity) became more secure than paper-based embodied-rights systems (which relied on the integrity of the signatories and the authenticity of the signatures.). Checks—the instruments most commonly used to transfer these accounts—became nonnegotiable in most of the civilized world, although they retained their ancient character in the United States.⁹⁶ This shift had occurred by the second half of the nineteenth century, well before the advent of the mainframe computer in the 1950s.

2. *Securities Transfers*

Money started with specie, progressed to embodied-rights tokens, and worked its way to accounts. The history of securities is more complex. Securities started in the seventeenth and eighteenth centuries as a jumble of account and embodied-rights systems.⁹⁷ The account system was strong in this era, with ownership predicated upon registration on the books of the issuer. This made sense in the eighteenth and even early nineteenth century, because securities are unlike money.

The holder of money is interested in instant transferability of an object of value. This is something provided by reliable tokens. The holder of securities—if a long-term investor—needs transferability less, but needs re-

93. Benjamin Geva, *From Commodity to Currency in Ancient History—On Commerce, Tyranny, and the Modern Law of Money*, 25 OSGOODE HALL L.J. 115, 117 (1987); see *Bank of United States v. Bank of Georgia*, 23 U.S. (10 Wheat.) 333, 346-48 (1825) (receipt of bank credit is payment).

94. An alert reader will spot circular reasoning here. This is true, but not to worry. Money—as a social consensus—is based on pure circular reasoning. I will accept a dollar bill as money only because you are willing to do so. See Sommer, *supra* note 66, at 11-19.

95. *Id.* at 12-19.

96. Gilmore, *supra* note 44, was among the first to argue that the legal system of negotiable debt instruments survived any use for these instruments. This is likely true, but the utility of other negotiable instruments—documents of title and securities certificates—still persists, albeit decreasingly so.

97. A brief history of early securities holdings can be found in Rogers, *supra* note 39, at 471-78.

liable dividends more. Dividends are not reliable unless the issuer knows where to send the money. Transferable securities tokens are therefore a nuisance—for issuers, at least. Sometimes, transferability even destroys the very purpose of securities, as with the securities of closely held corporations. It is no surprise that embodied rights were not dominant in the early world of securities transfer.

Negotiable securities certificates were latecomers that met the commercial demands of early twentieth-century America.⁹⁸ By this time, speculative holdings of equity stock—and often debt—were financed on margin. The financiers demanded clean and ready access to their collateral. The liquidity needs of the financiers would not suit the tedious registration requirement, especially in a national economy. Furthermore, holdings of securities became increasingly widespread, and brokers developed as intermediaries between investors and issuers.

The solution, perfected by the early twentieth century, was a peculiar hybrid. Equity securities certificates were negotiable property. These tokens did not signify a right to payment. Instead, certificates gave their holder a right to registration on the books of the issuer. In turn, registration conveyed the usufruct of the security. A broker could therefore retain the customer's certificate and finance it, with dividends and voting rights still belonging to the customer unless the broker foreclosed and exercised its right to register. Bearer debt securities followed the same rules as ordinary negotiable instruments. Because most corporate debt involved a stream of interest payments followed by eventual repayment of the principal, the certificate had a series of detachable coupons, collectible as negotiable instruments each payment period. Equities and debt finally received common treatment in UCC Article 8.⁹⁹

The commercial demands of late twentieth-century America required yet another shift—from embodied rights back to accounts. The shift—enabled by the computer—was forced by high transactional volumes that swamped paper-based systems. This securities account system was decentralized, involving various tiers of intermediaries, each of whom held for a lower tier. Part 5 of Revised UCC Article 8 finally gave formal recogni-

98. *Id.* at 476-77. These demands were real, but not overwhelming. In many countries, certificates never got off the ground, or were restricted to anonymous bearer instruments. However, American exceptionalism in the law of securities may be more than American legal quirkiness. Even in the early twentieth century, the United States had an extraordinarily rich and deep equities market.

99. See U.C.C. art. 8 prefatory note (1994).

tion to this tiered holding system.¹⁰⁰ One could call Part 5 a kind of “cyberlaw,” but it is also just another oscillation between well-established token and account systems.

Despite the shift to accounts, securities, money, or other account-based systems may yet return to embodied rights. “E-money” embodied-rights tokens certainly exist, although there is some question about their commercial viability. Any new embodied-rights systems would probably be registry-electronic or physical-electronic.¹⁰¹ (It is hard to see what advantages a new paper system would have in an electronic world.) But it is just as hard to see what is legally novel about these new systems. Their commercial law would resemble the old commercial law of tokens in fundamentals: preserving uniqueness and merging the legal claim with control of the authenticated token symbol.

C. E-Contract Formation and Electronic Agents

Upon reading UETA, one is impressed by its modesty. The spirit of UETA can be captured by passages such as: “A record or signature may not be denied legal effect solely because it is in electronic form” or “A contract may not be denied legal effect solely because an electronic record was used in its formation.”¹⁰² Much of UETA is not an attempt to prescribe what the law should be; it is a gentle reminder of what the law should not be.

UETA’s modesty becomes it. There is little new about electronic contract formation. In common law, contract formation is informal; a handshake will do as well as a signature. If the statute of frauds is satisfied (when relevant),¹⁰³ any act that manifests the assent of the parties is suffi-

100. Joseph H. Sommer, *A Law of Financial Accounts: Modern Payment and Securities Transfer Law*, 53 BUS. LAW. 1181 (1998).

101. See *supra* text accompanying note 89.

102. UNIF. ELEC. TRANSACTIONS ACT §§ 7(a)-(b), 7A U.L.A. 30 (Supp. 2000). Similar in spirit is UNCITRAL Model Law on Electronic Commerce, 36 I.L.M. 197 (1997), or the federal Electronic Signatures in Global and National Commerce Act (“E-Sign”). See *Electronic Signatures in Global and National Commerce Act*, S. 761, 106th Cong. (2000) (enacted). We discuss UETA in preference to E-Sign because UETA’s electronic contracting provisions are more comprehensive in scope. E-Sign does not preempt UETA, but contains some consumer protections not found in UETA. See *id.* § 102(a)(1)(A).

103. Courts have had 140 years of experience with the statute of frauds in cyberspace. *E.g.*, *Dunning & Smith v. Roberts*, 35 Barb. 463, 468 (N.Y. App. Div. 1862); *Trevor v. Wood*, 36 N.Y. 307 (1867) (statute of frauds satisfied by telegrams). *Trevor* also clearly stands for the proposition, enshrined in both UETA and E-Sign, that parties must consent to electronic commerce. Sixty years after *Smith*, the statute of frauds was a matter of course for telegrams. See 27 C.J. *Statute of Frauds* 307 n.33 (1922).

cient.¹⁰⁴ It may be easier to sign an electronic document without intending to do so,¹⁰⁵ but this problem exists in the paper world and is a traditional staple of consumer law. Many people sign without reading the fine print, just as others click without opening the link to the terms and conditions.

In contract formation, UETA presents only one new issue—contracting with machines that have something resembling discretion. People have long been forming contracts with vending machines.¹⁰⁶ Courts have not been fazed by such contracts,¹⁰⁷ probably because they have closely resembled ordinary “take-it-or-leave-it” consumer contracts. A sales clerk without discretion closely resembles a vending machine for many contractual purposes, although the sales clerk might resent the comparison and the machine would not. One thing, however, is new. Machines are sufficiently complex so that they are acquiring something that resembles discretion. In other words, the machine may produce a result not anticipated by the programmer or user. This kind of “mechanical discretion” seems genuinely novel, at least when applied to contracting machines. As we shall see, this genuine transactional novelty is amenable to traditional legal analysis, if we don’t push it too far.

These contract-forming machines—often software embedded in a computer system or transferred among computers—are often called “electronic agents.”¹⁰⁸ This term is usually a misnomer. A programmed machine is not a juridical person and therefore cannot be an agent. It can owe

104. Of course, not every act that *manifests* assent is a true act of assent. The law determines which acts correspond to assent regardless of the psychological state of the actor: the objective theory of contract formation. James J. White, *Autistic Contracts*, 45 WAYNE L. REV. 1693 (2000).

105. See, e.g., Cem Kaner, *The Insecurity of the Digital Signature*, at <http://www.badsoftware.com/digsig.htm> (Sept., 1997).

106. Vending-machine technology dates back to the late nineteenth century, but may have antecedents far more ancient. See *supra* note 11.

107. Several courts, following WILLISTON ON SALES § 242b (2d ed. 1924), have mentioned automats (a self-serve restaurant in which a person inserted a coin in a slot and took food out) with equanimity. See *Cushing v. Rodman*, 82 F.2d 864, 868 n.29 (D.C. Cir. 1936) (in implied warranty of fitness case for food, favorably citing Williston’s statement that vending through automat made no difference); *Child’s Dining Hall Co. v. Swingler*, 197 A. 105, 113 (Md. 1938) (Offutt, J., dissenting) (defective crab-cake sandwich, citing WILLISTON ON SALES § 242b (2d ed. 1924)); see also *Seattle v. Dencker*, 108 P. 1086, 1087 (Wash. 1910) (In police power case deciding that the state could not discriminate between sales by human and by vending machine, the court noted that vending machine at question had no greater ability to defraud consumers than other vending machines. “The cigars are at all times exposed to view under their proper labels and prices, so that the purchaser can at all times see what he is getting for his money, and he gets just what he pays for.”).

108. E.g., *infra* text accompanying note 112.

no duty of obedience. It simply responds to its internal programming and external parameters. Beyond its programming and parameters, it cannot keep its user informed of the transactions it is processing, or problems that might be developing. It cannot be sued, owes no fiduciary duties, and has no interests of its own. It cannot appear to be a principal thereby triggering the law of undisclosed principals: it is clearly a machine.¹⁰⁹ "Agent" is a well-understood legal term, based on underlying assumptions that have consequences. A machine cannot be an agent except by analogy. As will be shown, however, the analogy breaks down in many spots.¹¹⁰

Of course, a juridical person can conduct its agency exclusively through machines. An intermediary collecting bank in check law is a good example. An intermediary collecting bank uses a completely automated process: reading magnetic ink characters on checks, sorting the checks accordingly, and transmitting the checks and cash letters to the next bank in the chain. This automated processing is legally a sub-agency for the depositor of the check.¹¹¹ In other words, the intermediary bank is an agent, acting through solely automatic means. However, this is not the common legal meaning of the "electronic agent." As UETA puts it:

"Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.¹¹²

We already have two insights, both in the form of misnomers. An "electronic agent" is not really an agent, and "mechanical discretion" is not really discretion. We must stick with these terms, however. "Electronic agent," after all, is now a legal term of art.

UETA's definition of "electronic agent" is not only a misnomer, but also it does not tell us why an electronic agent is legally interesting. Section 14 of UETA fills this gap:

109. Note that this statement implies that the Internet itself is a kind of electronic agent. This is not inconsistent with UETA's definition of electronic agent: *infra* text accompanying note 112. For further discussion, see *infra* text accompanying note 128.

110. See *infra* text accompanying note 116; *infra* note 120; *infra* text accompanying notes 120-123; *infra* text accompanying note 128; *infra* note 133.

111. U.C.C. § 4-201(a) (1999). A check-processing system meets UETA's definition of "electronic" because checks use magnetic encoding. See UNIF. ELEC. TRANSACTIONS ACT § 2(5), 7A U.L.A. 20 (Supp. 2000) ("'Electronic' means relating to technology having electrical, digital, magnetic . . . or similar capabilities.").

112. UNIF. ELEC. TRANSACTIONS ACT § 2(6), 7A U.L.A. 20 (Supp. 2000).

In an automated transaction, the following rules apply:

(1) A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.

(2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.¹¹³

Think of a credit card swiped through a soda machine: a UETA "automated transaction." The swipe creates an obligation of the vending machine's owner to deliver a soda, and a series of obligations to pay through the credit card system. Or the obligation may be unilateral. For example, a coin placed in a vending machine creates an obligation to release the coin or deliver the goods.

A comment to section 14 explains matters further. The section "negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, *the requisite intention flows from the programming and use of the machine.*"¹¹⁴ In other words, "one simply disregards the autonomy demonstrated by the electronic device in the formation of the agreement and pretends that it is nothing more than a communication tool. . . . [W]e pretend that anything issuing from the computer really issues from its human controller."¹¹⁵ According to UETA, an electronic agent merely shifts human volition in time and space, and further up the causal chain. However, the volition remains the legally significant event, unaffected by the electronic agent's intermediation. UETA says that we must ignore the intermediating device, and concentrate on the volition. This result is certainly not novel; it has probably existed since the days of clockwork. For example, an observant Jew cannot control a light on Sabbath, but may set a timer on Friday afternoon that is programmed to control Sabbath lighting. The timer is certainly an

113. *Id.* § 14, 7A U.L.A. 37 (Supp. 2000).

114. *Id.* § 14 cmt. 1, 7A U.L.A. 38 (Supp. 2000) (emphasis added).

115. Ian R. Kerr, *Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce*, 22 DALHOUSIE L.J. 190, 220-21 (1999) (emphasis added).

“electronic agent,” in the UETA sense. Because the human volition occurred at an acceptable time, the timer’s subsequent action is irrelevant to Jewish law.

This sounds nothing like agency law. In agency law, the intent or volition of a disclosed principal is irrelevant, if the agent’s act is (apparently) within the scope of the agency.¹¹⁶ UETA, in contrast, views an electronic agent as a machine for manifesting assent. Therefore, attribution of the intent to the machine’s output is the key.¹¹⁷ Can the act of the “agent” be connected to the transactional intent of the “principal”?

The text of section 14 contains no attribution rules. The comment goes outside the text, stating that attribution is a matter of programming and use.¹¹⁸ But this is as far as it goes. Attribution is not always easy, and the drafters of UETA were probably aware of this. The programmer is not always the user, and might not even be the agent of the user. Unless the user and programmer are the same, the user almost certainly does not know the programmer’s intent, as expressed by the programming parameters. The program might not even reflect the programmer’s intent: software bugs. The user might not even know it is the user: consider a virus that emits messages in response to the user’s keyboard strokes, with the user having no knowledge of the virus or these messages.

Machine discretion has several dimensions. The drafters of UETA did not seek to tease these dimensions apart, and explain their analytical consequences. Instead, they left most of the process to an evolving common law, which may be safely codified after enough experience. We do not yet have the experience—an established case law—but a few hypothetical cases are very suggestive. The first three hypotheticals set the stage, illustrating some legal differences between agents and electronic agents:

The Haggling Agent: Suppose you want to buy a book in the bazaar, and must haggle the price. You do not do so yourself, but send a friend to act as your agent. The bookseller knows that your friend is acting as your agent. The bookseller quickly discovers that your friend is a poor negotiator. You only learn this when your friend buys the book for five times the price typically negotiated. In this hypothetical, the rights of the parties are clear. You owe the bookseller the full price, but may be able to sue your friend for lack of ordinary care.

The Haggling Slave: Same as the previous hypothetical, except your friend is replaced with your slave. A slave, in many legal systems, has no

116. RESTATEMENT (SECOND) OF AGENCY § 144 (1958).

117. See Kerr, *supra* note 115, at 222-37.

118. UNIF. ELEC. TRANSACTIONS ACT § 14 cmt. 3, 7A U.L.A. 38 (Supp. 2000).

legal personality and therefore cannot be an agent. Nevertheless, a slave certainly has human discretion. At least in the Roman system, a slave—although not an agent—could bind his or her master, under appropriate circumstances. Is the law of slavery, then, a legal template for the law of electronic agents?¹¹⁹

The Online Bookstore: You decide to buy a book on an online bookstore. The bookstore's website suggests a price, on a take-it-or-leave-it basis. (The price incorporates both past sales of the book, and your buying history.) You order the book, at five times the price you could have gotten elsewhere. On the strength of section 14(2) of UETA, you are bound by that price. You have no agent to blame, but only yourself.

The Hagglng Electronic Agent: You do not wish to comparison-shop, so you use your own electronic agent, which searches among the various bookstores. You licensed the agent from a software house, whose license terms contain a standard "as-is" clause. The bot orders your book from one of the online booksellers, at five times the price you could have gotten elsewhere. Thanks to the disclaimer, you have no claim against the software house, notwithstanding its poorly functioning software.¹²⁰ However, you may have a claim against the bookseller: a claim that would not exist if your electronic agent were governed by the law of agency (as in the "Hagglng Agent" hypothetical).

UETA tells us that an electronic agent provides mechanical manifestation of intent. A manifestation of intent does not necessarily make a binding contract, for example, if the intent were mistakenly manifested. "A mistake is a belief that is not in accord with the facts."¹²¹ As a consumer, you may have reasonably believed that the software would conform to your wishes. After all, notwithstanding the standard "as is" disclaimer, the

119. This insight can be found in Kerr, *supra* note 115, at 237-39. U.S. law seems discouraging on this score, denying any juridical capacity to slaves. *See* Hall v. United States, 92 U.S. (2 Otto) 27, 30 (1875) ("the slave was incapable of entering into any contract").

120. The software provider's "as-is" disclaimer of its warranty of merchantability is only effective because it is a licensor, not an agent. If the software provider were an agent, it would have to disclaim far more to avoid all liability. *See* RESTATEMENT (SECOND) OF AGENCY § 381 (1958) (duty to inform principal of problems with the software, e.g., discovered bugs); *id.* § 383 (duty to act only as authorized), 384 (duty not to try the impossible); *id.* § 385 (duty of obedience); *id.* § 387 (loyalty, e.g., no business relations with the bookseller); *id.* § 395 (nondisclosure of confidential information).

121. RESTATEMENT (SECOND) OF CONTRACTS § 151 (1981). The most comprehensive treatment of the doctrine of mistake of which I am aware is GEORGE E. PALMER, *THE LAW OF RESTITUTION* (1978). The problem of mistake occupies eight of the twenty-three chapters of this four-volume treatise.

product had gotten good reviews.¹²² Your belief was erroneous, but not negligent. “The theory upon which a document binds one who signs it, but who does not read it, is that either he accepts it whatever may be its contents, or that he has been careless in choosing his informant.”¹²³ You picked your software with reasonable care and therefore may fairly claim mistake.

The mistake is unilateral, so it does not alone provide a basis for a rescissory remedy.¹²⁴ However, the contract may nonetheless be avoided either if:

- 1) the bookseller knew (or should have known) that it was dealing with Delphi’s bots and had reason to know that Delphi’s bots would accept ridiculous offers,¹²⁵ or
- 2) if enforcement of the contract would be “unconscionable.”¹²⁶ *Restatement (Second) of Contracts* unconscionability is a far less imposing beast than UCC Article 2 unconscionability. A sufficiently bad price seems enough to trigger the *Restatement* threshold, if the rescissory remedy is not too harsh to the counterparty.¹²⁷

Therefore, it is possible to rescind the contract, return the book, and regain your purchase price under UETA and the law of mistake.

Procrustes Software: Understandably upset with your previous bot, you find a shopping bot with a warranty, provided by Procrustes Software. Procrustes’ bot is flawlessly programmed, exhaustively documented, and is guaranteed to never yield an unpredictable result. However, the user interface is very complex. You use the bot, but fail to notice that you had accidentally set the interface to find the highest price on the Internet,

122. If grilled by the bookseller’s counsel, you would have had to admit that you could not have been positively certain that the software would have worked as you had expected. But mistake is subjective: it is enough that you never contemplated the possibility of bugginess at the time, if your failure to do so was reasonable. See PALMER, *supra* note 121, § 16.8.

123. *Ricketts v. Pennsylvania R.R. Co.*, 153 F.2d 757, 760 (2d Cir. 1946) (concerning reasonable reliance on person’s lawyer’s representations as to contents of contract); *cf.* RESTATEMENT (SECOND) OF CONTRACTS § 154(b) (1981) (risk of mistake would be shifted if mistaken party was “aware, at the time the contract is made, that he has only limited knowledge with respect to the facts to which the mistake relates and treats his limited knowledge as sufficient.”); see PALMER, *supra* note 121, § 15.8.

124. RESTATEMENT (SECOND) OF CONTRACTS § 152 (1981).

125. *Id.* § 153(b).

126. *Id.* § 153(a).

127. *Id.* § 153 cmt. c.

rather than the lowest one. This hypothetical, of course, would be a classical application of the law of mistake. The only difference between this one and the one above is that the mistake occurs at the user level, rather than at the machine level.

Online Bookstore Redux: The “Online Bookstore” hypothetical did not involve any agents or bots: just a consumer and a bookstore. However, UETA insists that electronic agents were present. Your computer responded to your keystrokes “without [subsequent] review or action.”¹²⁸ The computer is an electronic agent, although it does not seem to possess any discretion. The bits fly over the Internet without review or action. The Internet is an electronic agent. These nondiscretionary electronic agents differ from the discretionary ones. They either work or they do not, and one of the parties is likely to be able to prove it without recourse to subjective intent. UETA explicitly recognizes these kinds of mistake without mechanical discretion. Section 10 of UETA refers to “a change or error in an electronic record.” An “error” is a human keyboarding mistake; a “change” is a straight data corruption. Within this scope, section 10 is fairly liberal in that there is no unconscionability test, and UETA presumes that rescission is not harmful to the counterparty, if the party claiming mistake does not use what it has ordered.

The interesting case remains that of mechanical discretion. But mechanical discretion, like a third party, is unnecessary to the law of mistake. Any kind of machine error or reasonably unanticipated result—even a simple failure amounting to “abuse of discretion”—may trigger this body of law.

The characteristic law of electronic agency may therefore be the law of mistake. But the common law of mistake is a troublesome one for electronic commerce. The law of mistake has an equitable feel to it:

The rules governing [mistake] have traditionally been marked by flexibility and have conferred considerable discretion on the court. . . . In part it has been due to the fact that the law of mistake was shaped largely by courts of equity which had broad discretionary powers. This characteristic of flexibility marks the rules stated in this Chapter, as is evidenced by such necessarily imprecise language as “materially” (§ 152), “unconscionable” (§ 153), and “bears the risk” (§§ 152, 153, 154). In addition, § 158 makes it clear that if these rules will not suffice to do sub-

128. UNIF. ELEC. TRANSACTIONS ACT § 2(6), 7A U.L.A. 20 (Supp. 2000), cited in full text accompanying note 112.

stantial justice, it is within the discretion of the court to grant relief on such terms as justice requires.¹²⁹

This is sensible in ordinary person-to-person commerce. As the *Restatement* tells us, "experience teaches that mistakes are the exception and not the rule"¹³⁰ An improvident act is not a mistake; an erroneous prediction is not a mistake; acting knowingly on insufficient information is not a mistake.¹³¹

However, mistakes appear to be common in electronic commerce. They may occur whenever an electronic agent produces an unanticipated response. If we apply the *Restatement* to electronic commerce, every bad bargain becomes potentially avoidable because the elements of mistake are usually possible to plead. Because lawyers are trained to believe in enforcing bad bargains (unlike ordinary human beings),¹³² the result seems jarring.

Software is not human, however. Most of us likely know more of each other than we know of our machines. The argument for allocating risk on an unsophisticated user is therefore comparatively weak. The law of mistake is likely to place the risk of misunderstanding on the sophisticated counterparty of an unsophisticated user. (If both parties are sophisticated, the risk of misunderstanding is likely to remain with the user.) The sophisticated party will therefore have an incentive to ensure that the unsophisticated party, if using an electronic agent, understands what it is doing.¹³³ There is nothing novel about such indirect risk-allocation mechanisms. The credit card system uses a similarly indirect risk allocation for fraud. This risk is primarily assumed by the credit card system, rather than the card holders. It works quite well, because the credit card system is better at detecting fraud than most holders are at preventing fraud.

Finally, my treatment of the law of mistake is implicit in UETA, and provides a reasonable solution to many problems of electronic commerce.

129. RESTATEMENT (SECOND) OF CONTRACTS ch. 6 introductory note.

130. *Id.* § 155 cmt. c.

131. *Id.* § 151 cmt. (1981).

132. See STEPHEN VINCENT BENET, *THE DEVIL AND DANIEL WEBSTER* (1937); WILLIAM SHAKESPEARE, *THE MERCHANT OF VENICE*.

133. Professor Kerr gets to a similar conclusion, albeit through the law of agency, and its treatment of undisclosed principals. Kerr, *supra* note 115, at 246-47. (Agency differs from mistake, however. Agency would permit the rescission of a reasonable transaction: unilateral mistake only permits rescission of an unconscionable one.) Kerr demonstrates that the law of agency often yields a sensible result for electronic agent problems. This is true, but the law of agency often leads to the wrong result. See *supra* note 110. The law of mistake, however, gives a reasonable answer both where agency works and where it does not.

However, the law of mistake (or UETA) may not work in all contexts, and the mature law of machine discretion might look very different than this tentative exploration. Our speculations should not get too far ahead of our case law, and we do not yet have enough case law to support much further speculation.

D. Licensing of Software and Information

Today, most discussions of software and information licensing involve the Uniform Computer Information Transactions Act (“UCITA”), formerly known as proposed UCC Article 2B.¹³⁴ UCITA covers licensing of software and of much information in digitized form, although it does not cover the same information in paper form.¹³⁵ As of the time of writing, enactment in most states is very uncertain.¹³⁶ A detailed analysis of UCITA might therefore not be worth making, unless one wanted to persuade a legislature of the merits or defects of this statute. However, such an analysis is not to my purpose. Rather, I wish to show that UCITA—and thus software licensing in general—have long antecedents.

The skeleton of UCITA—the parts in which the sections are segregated—is a very familiar one. It would be identical to that of draft Revised Article 2, except that UCITA breaks out the warranties into a separate part.¹³⁷ This similarity is an historical artifact—the two statutes started out as part of a single “hub-and-spoke” statute,¹³⁸ and the drafters of UCITA retained the Article 2 organization when the two statutes became separate. However, it suggests that the licensing of information is not that analytically different from the sales of goods.

Of course, a license is not a sale, and information is not a tangible good. Sellers alienate their entire bundle of property rights (for a price); licensors prefer to retain some rights associated with the bundle. The common law of chattel property governs tangible goods; statutory intellectual property law usually governs information. The rules in Article 2 and UCITA are therefore going to differ. But these different bodies of law

134. See UNIF. COMPUTER INFO. TRANSACTIONS ACT (2000).

135. See *id.*

136. UCITA and UETA were both promulgated at the July, 1999 meeting of the National Conference of Commissioners of Uniform State Laws. Since then, UETA has been enacted by twenty-three states; UCITA by only two. See <http://www.nccusl.org/uniformacts-subjectmatter.htm> (last visited Nov. 12, 2000).

137. UCITA comes from the 2000 Official Text. Revised Article 2 comes from the 2000 Approval Draft (which was not approved).

138. See John A. Chanin, *The Uniform Computer Information Transaction Act: A Practitioner's View*, 18 J. MARSHALL. J. COMPUTER & INFO. L. 279, 279-80 (1999).

share the same skeleton. Cyberspace does not change the broad rules of a market economy for things of value, nor should it be expected to do so.

The two bodies of law nonetheless substantially differ in their details, as they should. The question for now is whether UCITA contains anything fundamentally “new”: either in Article 2 or in the common law of licensing. The answer appears to be “not much.” UCITA’s treatment of authentication, records, and electronic contracting—although more prescriptive than that of UETA—is nothing new, for all of the reasons discussed in the previous subsections.

UCITA does facilitate the creation of intellectual property rights from contractual cloth.¹³⁹ This idea, although very controversial, is scarcely new. Covenants not to compete have been around at least since the eighteenth century.¹⁴⁰ Stock and commodities exchanges, by binding their members to agreements, have long treated price information as property.¹⁴¹ Similarly, contractual arrangements within press associations have

139. As one example, UCITA legitimates enforceable click-through licenses. Because the relevant software or information cannot be accessed without manifesting assent on these licenses, it is impossible to use the information or software without a legal relationship with the licensor. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 112(d) (2000) (“Conduct or operations manifesting assent may be shown in any manner, including a showing that a person or an electronic agent obtained or used the information or informational rights and that a procedure existed by which a person or an electronic agent must have engaged in the conduct or operations in order to do so.”). This may formally be characterized as a contract between licensor and licensee. However, as an operational matter, it is nothing but a property right of the licensor, valid against the world. For some reason, UCITA insists that it does not create property rights. *See id.* § 102(a)(38) (defining “informational rights,” as arising from any “law that gives a person, *independently of contract*, a right to control or preclude another person’s use of or access to the information on the basis of the rights holder’s interest in the information.”) (emphasis added). *But see id.* § 112(d) (referring to “information or informational rights” as subject of license). Perhaps the UCITA drafters fear the Supreme Court’s jealousy of federal intellectual property law. *See infra* cases cited in note 312. But this fear, even if it were a motivating factor, may be misplaced. *See infra* text accompanying notes 140-142.

140. *See, e.g.,* *Mitchel v. Reynolds*, 24 Eng. Rep. 347 (K.B. 1711) (holding that “a bond or promise to restrain oneself from trading in a particular place, if made upon a reasonable consideration, is good.”).

141. *See* J. Harold Mulherin et. al., *Prices are Property: The Organization of Financial Exchanges from a Transaction Cost Perspective*, 34 J.L. & ECON. 591 (1991). According to these authors, the New York Stock Exchange had begun restricting dissemination of price information as early as 1817. *Id.* at 597. The invention of the stock ticker in 1867 put this problem on a more formal and modern footing. *Id.* at 606. The intellectual property issue was first fully joined in *National Telegraph News Co. v. Western Union Telegraph Co.*, 119 F. 294 (7th Cir. 1902). (This case dates the stock ticker at 1881. *Id.* at 295.) However, the same results were reached by earlier courts, albeit on a contractual or fiduciary theory rather than a property theory. *See, e.g.,* *Telegraph Co. v. Gregory*, 1896

long treated hot news as property, although the news itself could not be copyrighted.¹⁴² Secrecy has long been a form of intellectual property. Courts have enforced all of these rights, albeit often with more restrictions than UCITA would impose.

As another controversial practice, UCITA seeks to legitimize the “shrinkwrap license”: a deemed manifestation of assent that may occur whenever the offeree is warned that a particular act will constitute assent, even if the terms are unknown to the offeree.¹⁴³ There are no new legal developments here. The revolution—if any—occurred with Llewellyn’s old Article 2, which abandoned most formalisms of contract formation, and sought a contract wherever it could be found.¹⁴⁴ Arguably, Llewellyn was merely traveling the path blazed by Lord Mansfield, inventor of quasi-contract and restitution.¹⁴⁵ Professor White reminds us that the old “objective” theory of contract formation is perfectly consistent with shrinkwrap licensing.¹⁴⁶

As Judge Easterbrook pointed out, many traditional contracts—tickets, insurance policies—involve payment before contract formation.¹⁴⁷ “Shrinkwrap licenses” are not even peculiar to software licenses: mail-order goods are often shipped with the sales contract in the shipping container. Modern courts have no problem finding a contract with these agreements, although not always on the terms specified by the shrinkwrap.¹⁴⁸ This is really the only disagreement in the shrinkwrap licensing

Q.B. 147. The Supreme Court soon followed the Seventh Circuit’s approval of this new intellectual property right. *Board of Trade v. Christie Grain & Stock Co.*, 198 U.S. 236, 250-51 (1905).

142. *See Int’l News Serv. v. Associated Press*, 248 U.S. 215, 237-239 (1918).

143. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 112 (2000). As a general rule, the offeree must have an opportunity to review the terms before being bound, or the offeree will have a right to rescind, but not always. *Id.* § 112(e)(3)(B).

144. *See U.C.C. §§ 204-09* (1999) (eliminating some common law consideration requirements and the requirement that the acceptance mirror the offer).

145. *See Moses v. Macferlan*, 97 Eng. Rep. 676 (K.B. 1760). Lord Mansfield may have been a mere prophet of restitution; the American Law Institute might be the true inventor. *See Andrew Kull, Rationalizing Restitution*, 83 CALIF. L. REV. 1191, 1192 (1995).

146. White, *supra* note 104.

147. *Pro-CD v. Zeidenberg*, 86 F.3d 1447, 1451 (7th Cir. 1996).

148. For example, some courts have treated pay-before-assent shrinkwrap licenses as classic “battles of the forms.” *Step-Saver Data Sys., Inc. v. Wyse Tech.*, 939 F.2d 91 (3d Cir. 1991); *Arizona Retail Sys., Inc. v. The Software Link*, 831 F. Supp. 759 (D. Ariz. 1993). Other courts (and UCITA) have treated them as enforceable, subject to a right of return. *Pro-CD*, 86 F.3d at 1447; *M.A. Mortenson Co. v. Timberline Software Corp.*, 998 P.2d 305 (Wash. 2000.)

controversy: do the terms of the shrinkwrap—delivered post-formation—govern, or may a court choose to ignore these terms and fill in its own? The contract exists, in either case.

There may be only one place where UCITA is genuinely innovative: its notion of “mass-market transaction.” (Even here, the notion seems to be part of English law.)¹⁴⁹ In essence, this notion is that of a standardized license “directed to the general public as a whole.”¹⁵⁰ A mass-market license is offered on the same basis to everybody: consumers, merchants, and cats. The ideal type mass-market transaction is the boxed set of software sold to companies and consumers alike. This idea could just as easily have been placed in Article 2: a mixture of consumer and nonconventional commercial law, of undisputed elegance but uncertain utility.

E. A Final Word on Electronic Commerce

In conclusion, little is new about the law of electronic commerce. The law of records and messages will continue to serve its traditional functions, with only modest doctrinal changes. The old doctrine may, however, be expressed in a more precise legal language, without the hidden assumptions embedded in paper media. Embodied-rights and account systems will continue to compete with each other, as they have for the past few centuries. Electronic contracting introduces the notion of “electronic agency,” which, when conjoined with “machine discretion,” is about the only substantially new legal development on the list. But despite the novelty of the legal problem, the old law of mistake seems to fit matters nicely. Finally, licensing of information has been a traditional legal practice (although—as will be seen—the intersection between modern licensing practice and copyright law may be novel). Any new ideas introduced by UCITA could apply equally well to sales of goods, and could have been introduced fifty years ago.

This should be no surprise. Most of “electronic commerce” is not particularly novel. Electronics has been a handmaiden to commerce ever since the telegraph. The law of electronic commerce has also been around since at least the 1860s and has been the topic of legal analysis since at least the 1920s.¹⁵¹

149. See Charles Proctor, *International Banking and Unfair Contract Terms*, 14 BUTTERWORTH'S J. OF INT'L BANKING & FIN. L. 6, 230 (1999) (describing the Unfair Contract Terms Act of 1977).

150. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 102(a)(46)(B)(i) (2000).

151. See *supra* note 103 (early telegram cases and analysis); Young B. Smith, Note, *Liability of a Telegraph Company for Transmitting a Defamatory Message*, 20 COLUM. L. REV. 30, 369 (1920); 62 C.J. *Telegraphs and Telephones* (1933). The *Corpus Juris*

IV. NO DOCTRINAL REVOLUTION: THE LAWS OF SOVEREIGNTY

The Internet is the luminiferous ether of the age: pervading everything, yet tangible nowhere. The original luminiferous ether lost its luster in 1905, when Einstein invented special relativity. Even if the Internet avoids that fate, it must still deal with the troublesome persistence of sovereignty. How does a medium without borders coexist in a territorial polity? How does a supranational order cope with territorial boundaries? How do autonomous communities survive if embedded in a polity not defined by the community? These questions are at least as old as the Holy Roman Empire. Yet the relationship between the Internet and sovereignty is a popular theme in the cyberlaw literature.¹⁵² Is anything new today?

On a more humble level, the conflict of laws seeks to deal with the same problem: the overlaps of multiple sovereignty. (Civilians call this field "private international law.") This field encompasses at least three bodies of law: the law of jurisdiction, choice of laws, and the law of enforcement of judgments. The classic conflicts paradigms are intensely physical: an automobile accident, a failed marriage, a shipment of goods, and a person's death.¹⁵³ Conflicts law must somehow assert the relevance of territorial sovereignty over a borderless medium. Is this possible?¹⁵⁴

article reads like an early essay in the law of electronic commerce, with section headings such as "Transmission of Money," "News, Ticker or Market Quotation Service," and "Wire Tapping, and Opening Messages Addressed to Another." Sections include titles such as "Profane, Indecent or Obscene Language," "Furtherance of Gaming Transactions," and "Messages Related to Contracts."

152. The *Indiana Journal of Global Legal Studies* produced a symposium on this topic in 1998, as did the *Chicago-Kent Law Review* in 1999. See *Developments—The Law of Cyberspace*, 112 HARV. L. REV. 1574 (1999). Other articles and books on this subject are discussed below.

153. See *Neumeier v. Kuehner*, 286 N.E.2d 454 (N.Y. 1972) (major choice-of-law case on automobile accidents); RESTATEMENT (SECOND) OF CONFLICTS OF LAW §§ 285-86, 233-34, 257-59 (1969) (law governing divorce and annulment; law governing marital property); *id.* § 191 (shipment of goods); *id.* §§ 314-66 (decedent's estates).

154. This issue has been the subject of a fair amount of commentary. See, e.g., David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J.L. & TECH. 3 (1996); BORDERS IN CYBERSPACE (Brian Kahin & Charles Nesson eds., 1997); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993 (1994); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1 (1996); Geist, *supra* note 27; Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution*, 38 JURIMETRICS J. 575 (1998); American Bar Association Global Cyberspace Jurisdictional Project, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet* (Draft) [hereinafter ABA Report], <http://www.abanet.org/buslaw/>

This section discusses the issues posed by borderless media and borderless communities in a world of multiple territorial sovereigns. It concludes that some of these issues are old and insoluble; others are old and successfully solved. Nothing changes when the borderless medium is the Internet, or when the borderless communities are users of the Internet. Things have been borderless long enough: what matters is sovereignty.

A. Sovereignty, Governance, and the Internet

The problems concerning sovereignty and the Internet are a subset of a more general issue: how does the law of a state deal with communities not defined by that state? How do such communities govern themselves? These problems are old ones with many manifestations. The Internet is merely another battleground for some old wars.

This Article takes two approaches to these issues. First, it looks at the relationship between virtual communities and the state, which is characterized by cooperation rather than either irreconcilable conflict or rigid separation. Second, this Article emphasizes that the debate surrounding the roles, scopes, and limits of the public and private sectors is very traditional in legal circles.

1. *Internet versus State: The Johnson-Post Assertion*

The conflict between the Internet and the state is framed by a very significant 1996 paper by David Johnson and David Post. The paper argues that cyberspace is a community of its own, governed by norms of its own, independent of the law of the state.¹⁵⁵ Johnson and Post—at one end of the debate—conclude that the state should not be involved in cyberlaw.¹⁵⁶

cyber/initiatives/jurisdiction.html (last visited Nov. 26, 2000); *Developments, supra* note 152, at 1680-1703.

155. Johnson & Post, *supra* note 154. The sentiment may have originally come from John Perry Barlow:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

Developments, supra note 152, at 1681 n.6.

156. This normative statement has a positive counterpart: cyberspace is unregulable by the state, presumably because of cryptography and the structure of the Internet. Several authors have challenged this assertion. *E.g.*, Goldsmith, *supra* note 40; LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999). *See also infra* note 262 and accompanying text. What little I have to add may be left in the margin. Most of what occurs in the Internet is commercial. Most commercial transactions require payment in money. *Bank money is auditable; all Internet money is bank money; all banks are regulated.* Therefore, the commercial part of the Internet—most of the Internet—is regulable

This extreme position, although routinely attacked by most subsequent authors,¹⁵⁷ nicely frames the challenge the Internet poses to sovereignty.

The Johnson and Post argument first assumes, reasonably enough, that cyberspace is a transnational autonomous community or communities.¹⁵⁸ The word “community” is certainly vague enough to support such an assumption, and cyberspace is certainly transnational. Nor is the “autonomy” assumption problematic. Much conduct on the Internet, like the rest of civil society, is governed by norms of its own, independent of the law of any sovereign. The non sequitur comes with the next step. Johnson and Post assume that because a transnational autonomous community is governed by norms of its own, it does not need the intervention of the state. This jump looks implausible when placed in context. There are many voluntary self-governing communities including religious communities, private associations, corporations, and law merchant communities.¹⁵⁹ Many of these communities are multinational and have long histories. The multinational corporation, for example, dates to the beginning of the twentieth century.¹⁶⁰ Multinational religious communities are at least as old as the Catholic Church; the correspondent banking network dates back to the Renaissance. Many of these communities—even the international or virtual communities—derive strength from the state.

through the money. My key assertions (italicized) may need some amplification. Bank money is not inherently auditable, but this is a choice of the regulators. Second, although some issuers of Internet money are not chartered as banks, they are nevertheless regulated. See NATIONAL CONFERENCE OF COMMISSIONERS OF UNIFORM STATE LAWS, UNIFORM MONEY SERVICES-BUSINESS ACT (Aug. 4, 2000), <http://www.law.upenn.edu/bll/ulc/moneyserv/msb0620.htm>; 18 U.S.C. § 1961 (1994) (criminalizing the illegal transmission of money). One could argue that the Internet could set up its own alternative banking system, free of the state. Cf. FRIEDRICH HAYEK, *THE DENATIONALISATION OF MONEY* (2d ed. 1978). But if this were true, drug lords would have done so long ago. But they have not, because they cannot. Banking is a network industry of trust. The network is overwhelmingly regulated, much of the trust *comes* from state regulation, and the barriers to entry are far too high.

157. This began with a companion-piece in the same issue of the *Stanford Law Review*. See Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996). For a list of citations, see Wu, *supra* note 27, at 1194 n.78. For a particularly sophisticated analysis, see Margaret J. Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295 (1998). For a particularly amusing (and incisive) analysis, see Timothy Wu, *When Law and the Internet First Met*, 3 GREEN BAG 2d 171 (2000).

158. *Developments*, *supra* note 152, at 1586-1609.

159. Henry H. Perritt, Jr., *Cyberspace Self-Government: Town-Hall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413, 451-63 (1997).

160. See ALFRED D. CHANDLER, JR., *SCALE AND SCOPE: THE DYNAMICS OF INDUSTRIAL CAPITALISM* (1990).

The international banking community, of ancient lineage, is a good example of such a "virtual community." The virtual credentials of bankers—dematerialized, international, and networked—are as good as anybody's and far older. Bankers' stock in trade is nothing but authenticated symbols, mostly maintained and transmitted in electronic form.¹⁶¹ Banking is international, and has been so since the Renaissance. Banking is a quintessentially networked activity: a bank with no correspondents is no bank at all.

To be more specific, consider the banker's letter of credit: an ancient corpus of international practice. The letter of credit community is distinct, governed by norms of its own, independent of the law of the state. The bankers have even codified their norms in the Uniform Customs & Practice for Documentary Credits ("UCP") of the International Chamber of Commerce or the International Standby Practices ("ISP").¹⁶² These norms lend themselves to self-enforcement, often through preclusion rules. Johnson and Post's salient concept—autonomous self-governance in an international setting—is present here, without the Internet.

Most states have nonetheless subjected this community to municipal law, governed by reasonably appropriate conflict-of-laws rules.¹⁶³ The letter of credit community does not complain. This law establishes a needed framework of enforceability (and occasionally, unenforceability), and is sensitive to the needs of bankers and their customers. The international norms of the UCP and ISP are valorized in municipal law, which hearkens back to standard mercantile practice.¹⁶⁴ The international harmonization of this law, coupled with the choice-of-law rules, permits an autonomous international community to flourish in the shadow of municipal law.

The law of the state can respect autonomous governance as well as internationalization. Contract respects and regulates the autonomous governance of two parties. The difficult issues concern autonomous *multilateral* governance. This is common on the Internet, but such issues are common elsewhere. What else is a firm but autonomous governance of a large number of actors? One could argue that firms are generally hierarchical, and the Internet is an example of a more egalitarian autonomous

161. "Money is (carefully regulated) talk." Sommer, *supra* note 66, at 7. *Cf.* discussion *supra* notes 88-101 and accompanying text.

162. International Chamber of Commerce, Uniform Customs and Practice for Documentary Credits, ICC Pub. 500 (1993), <http://www.iccwbo.org/home/banking/778rev9.asp>; Institute of International Banking Law & Practice, International Standby Practices (1998).

163. *See, e.g.*, U.C.C. § 5-116(b) (1999).

164. U.C.C. §§ 5-108(e), 5-116(c) (1999).

multilateral governance. Yet even if this argument is accepted, bankers again provide a precedent: the “clearing house rules” of the Uniform Commercial Code. These rules, which go by several different names,¹⁶⁵ are promulgated by recognized groups of financial institutions, not individual institutions. They have the extraordinary power to bind those who do not specifically assent and to trump rules set forth in the UCC itself, including rules that cannot be varied by the parties through a bilateral agreement.¹⁶⁶ They do not, however, represent a complete cession of law-making power to the private sector. Financial institutions, being heavily regulated, are scarcely unconstrained members of the private sector.

Note that these clearing house rules are not only legal, regulating rights. They impose themselves on operations as well, limiting the operational possibilities of participants of the system without regard to the participants’ formal rights. This theme—familiar to anybody who has used an ATM machine—becomes no more astonishing or problematic when noticed on the Internet.¹⁶⁷ Clearing houses—and their operational restrictions—are old, dating back to the eighteenth century if not before.

The bankers show us that the problem of autonomous or transnational communities is an old one, often resolved satisfactorily. Private governance can coexist with statal government. Even when left unresolved, the problem recurs in many contexts apart from the Internet. Some of these contexts, such as banking, have a large “cyber” component; others, such as the legal problems posed by multinational business entities, are perhaps less virtual, although equally international. Some contexts—private standard-setting comes to mind—while neither necessarily virtual nor international, are still autonomous, interesting, and problematic.¹⁶⁸ Considering the large number of transnational and autonomous communities (including some—like banks—situated in cyberspace a century before the Internet), it

165. “Clearing house rules” in U.C.C. § 4-104(a)(4) (1999); “funds-transfer system rules” in U.C.C. § 4A-105(a)(5) (1989); “clearing corporation rules” in U.C.C. § 8-102(a)(4) (1999); *cf.* U.C.C. § 5-116(c) (1999).

166. U.C.C. §§ 4-103(b) (1999) (assent of parties bound not necessary), 4A-501(b) (1989) (assent not necessary; even most nonvariable rules of Article 4A can be varied), 8-111 (1999) (assent not necessary, all Article 8 rules can be varied.). *Cf.* N.Y.U.C.C. § 5-102(4) (McKinney 1999) (New York nonconforming provision abdicating U.C.C. rules if UCP is adopted, replaced by revised Article 5 in 2000.).

167. The literature on this is fairly extensive. For two examples, see Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998), and Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629 (1998). What may be new is the effect of these operating restrictions on intellectual property law. Of this, see *infra* Part V.B.

168. See *infra* text accompanying notes 199-200.

is difficult to understand the current dominance of the Internet strand of literature.

Let us conclude with Johnson and Post's specific contention: the law of the state cannot coexist with cyberspace. I have argued that their assertion relies on a non sequitur: that an autonomous community cannot tolerate a statal role. However, a non sequitur is not necessarily wrong. Even if some autonomous communities flourish in the shadow of the state, others may not. For example, the law of the state can kill a religious community.¹⁶⁹ Is the Internet community quasi-religious? In part, perhaps. But in general, probably not. The genesis of the Internet was in the Department of Defense, and the business of today's Internet is business. Even most of the nonbusiness Internet communities can live with the state, as Professor Lessig's recent book demonstrates.¹⁷⁰

2. *Internet and State: The Public-Private Dichotomy*

Though the Johnson and Post assertion may be largely incorrect, it has been very productive. A recent and sophisticated descendent of the Johnson and Post assertion is the concept of the Internet as a regulatory device: both autonomous of and linked with the state.¹⁷¹ This argument, along with the Johnson and Post assertion, gives primacy to the Internet as its own source of rules and norms. In contrast to Johnson and Post, this position does not deny a role for government, but rather stresses the continuity between Internet and state sovereignty.

This strand of literature emphasizes that the structure of the Internet is a social choice, not a technological necessity. The constraints and freedoms of the Internet are therefore also social choices. Governments or system architects may make centralized and conscious choices, akin to conventional regulation. Decentralized users, system architects, or even governments may also make choices that resemble market choice, either conscious or otherwise. Choice may be limited through norms, imposed as rules, or foreclosed by direct constraints on others' action. The Internet is a network: all choices affect others' opportunity sets, and therefore regulate the conduct of others. In this world, nongovernmental collective ac-

169. See Robert Cover, *Nomos and Narrative*, 97 HARV. L. REV. 4 (1983).

170. LESSIG, *supra* note 156.

171. The most significant manifesto of this literature is LESSIG, *supra* note 156. See also Riedenberg, *supra* note 167; Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 71 U. COLO. L. REV. 1263 (2000); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, 66 U. CIN. L. REV. 177 (1997).

tion resembles public regulation, the individual action of key players resembles collective action, and conscious choice competes with an impersonal market. On the Internet, the conventional categories of public (i.e., statal) and private (nonstatal) seem analytically thin—somewhere between irrelevant and pernicious.

The insights in the previous paragraph have spawned some of the most interesting of the cyberlaw literature: some fascinating studies of the private-public divide.¹⁷² But the previous paragraph was written very abstractly. Make a few word substitutions, and it describes far more than cyberspace: shopping centers,¹⁷³ the workplace,¹⁷⁴ homeowners' associations,¹⁷⁵ stock exchanges,¹⁷⁶ churches,¹⁷⁷ standard-setting organization,¹⁷⁸ and maybe any substantial collective human activity.¹⁷⁹ In all of them, the non-state actor regulates much like the state. Disobey the rules: suffer the consequences. The non-state's enforcement mechanism is different, using private shunning rather than public recourse to the state's monopoly of legitimate violence. Outside of a perfect atomistic market, shunning can be severe, including loss of livelihood or defining social contacts. Even the distinction in enforcement blurs: states can shun, and "private" legitimate violence is not unknown.¹⁸⁰

The cyber-commentators appreciate this argument; yet they still seek to distinguish their niche from the others. They succeed, as they must. Cyberspace is not the same as shopping centers, workplaces, or stock ex-

172. The public-private divide is an old field, subject to swings in fashion. See Christopher D. Stone, *Corporate Vices and Corporate Virtues: Do Public/Private Distinctions Matter?*, 130 U. PA. L. REV. 1441, 1441 (1982).

173. Compare, e.g., *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp.*, 650 A.2d 757 (N.J. 1994) (New Jersey constitution makes shopping center a public forum for free speech), and *Robins v. PruneYard Shopping Ctr.*, 23 Cal. 3d 899 (1979) (holding the same in California), *aff'd*, 447 U.S. 74 (1980), with *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972) (shopping centers private property for Federal Constitution).

174. See Charles A. Reich, *The Individual Sector*, 100 YALE L.J. 1409, 1423-26 (1991).

175. See Robert C. Ellickson, *Cities and Homeowners Associations*, 130 U. PA. L. REV. 1519 (1982).

176. Compare *Silver v. NYSE*, 373 U.S. 341 (1963) (using antitrust to import due process for broker violating system rules who was punished by exchange self-help), with *United States v. NASD*, 422 U.S. 694 (1975) (being subject to regulatory scheme connotes antitrust liability).

177. U.S. CONST., amend. I.

178. See *infra* notes 197-200.

179. See Reich, *supra* note 174, at 1429 ("Large organizations are governmental in nature, and government itself is just another large organization.").

180. See David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165 (1999).

changes, but the distinction tells us little. A distinction is not enough: the distinction must make a difference. Is cyberspace different from these other spaces in a way that is relevant to the public-private divide?

My thrust has a stock parry: the centrality of “code” in cyberspace. The private regulators of cyberspace—content providers and service providers—have information and access. Users want it, but physically cannot get it except with the aid of these regulators, who control the relevant “code.” These regulators may condition their aid as they choose; such is the power of “code.” Code, therefore, is a direct power of regulators to limit the possible choices of system participants within the system. (“Code” is another misnomer. As used here and in the literature, it includes constraints as tangible as prison cells.) This power is often unappreciated, possibly because it is either viewed as a necessary technological constraint, or as something natural: “the way things work.” It is frequently neither, but instead a conscious choice imposed on users.

This parry is a good one, but is open to rebuttal. Regulation through code is not limited to cyberspace. Workplaces, for example, have their own share of code: locked doors, ID badges and card readers, secrets (“information is power”), and the like. Some forms of regulation are extremely code-dependent. Consider roads, whose construction probably affects driver behavior more than posted signs and police cruisers. Or consider an airport and start counting the physical constraints on your action: speed bumps, parking lots, one-way tire shredders and escalators, metal detectors, baggage checks, tickets, gates, tiny seats, and a host of other affronts to one’s dignity.

Maybe the Internet is distinguished by a unique dependence on code as its premier regulatory device? No. As we have seen, airports use a lot of code. But the code of airports is physical, possibly far less plastic than the code of the Internet.¹⁸¹ Maybe the plastic code of the Internet is a distinction that amounts to a difference? Maybe. But even if it is, the Internet is scarcely unique or new. The code of banking is very similar to the code of the Internet: mostly restricted access to electronic data processing systems. As discussed a few paragraphs above, the banking system is difficult to distinguish from the Internet and has been around for quite a while.¹⁸²

181. One could question the plasticity of much Internet code. To the extent that decentralized users rely on protocols that have switching costs, the protocols lose their plasticity. The QWERTY typewriter keyboard is the classic example. Examples are easy to find in real computer code as well. As of the time of this writing, Microsoft has not yet abandoned the last vestiges of the obsolete DOS operating system in its new consumer operating systems.

182. See *supra* note 167 and accompanying text.

The quasi-regulatory nature of system rules is old hat in the banking industry. So is the corollary of system rules: the parastatal role of collective action in the “private” sector. Fifty years ago, commentators voiced concern about the private regulation implicit in Article 4’s recognition of clearing house rules, namely that it might be “unconstitutional as an improper delegation of legislative power to private interests”¹⁸³

Of course, banking is regulated. But then again, so is the Internet. The Internet Corporation for Assigned Names and Numbers¹⁸⁴ (ICANN) might not be New Deal style command-and-control regulation, but it is a fine example of Progressive-era regulation—an old-fashioned federal instrumentality, albeit one with international scope. The New Deal agencies such as the SEC seem to be filling their cyber-gaps¹⁸⁵ once they think they have some notion of what they are regulating. True, the Internet is not as regulated as banking. But such regulation may come once a consensus on regulatory goals and means develops.

In summary, many “private” actors—including those who comprise the Internet—remarkably resemble state actors. In a meaningful way, both regulate. Public and private regulation differ somewhat. The public sector is relatively more reliant on the state’s semi-monopoly of legitimate violence: the threat of police and prisons. The private sector usually uses shunning as its threat and punishment. Public and private regulators both also use “code”: the physical (including logical) constraints on the actions of regulated persons that were discussed above.¹⁸⁶ Code is regulatory, but unlike shunning or violence, works *ex ante* and often appears “natural.” The Internet, of course, is distinct from other venues. However, this distinction does not yet appear to make a difference.

3. *The Public-Private Distinction and Legal Doctrine*

At least four bodies of law govern the public-private divide. First, the state action doctrine places constitutional constraints (particularly Due Process Clause and First Amendment constraints) on public-sector ac-

183. Grant Gilmore, *The Uniform Commercial Code: A Reply to Professor Beutel*, 61 YALE L.J. 364, 375-76 (1952).

184. ICANN is a global non-profit association that oversees and administers policy for the naming and addressing of Internet sites. It is responsible for managing the Domain Name System [DNS] on an ongoing basis. It also acts as an arbitrator when disputes arise over a domain name’s ownership. See ICANN, *About ICANN*, at <http://www.icann.org> (last visited Nov. 26, 2000).

185. See, e.g., *infra* note 247 and accompanying text.

186. See *supra* text accompanying notes 181-183.

tors.¹⁸⁷ Second, the nondelegation doctrine adverted to earlier—which prohibits exercise of certain public powers by the private sector—is complementary to the state action doctrine.¹⁸⁸ The state-action doctrine makes certain private actions the equivalent of state actions: the nondelegation doctrine forbids private parties from conducting certain state actions. We do not discuss the nondelegation doctrine further, because it has long been in desuetude in federal law.¹⁸⁹ Third, the law of antitrust regulates non-state actors who have acquired the quasi-statal power to shun. Fourth, the First Amendment freedoms of speech and exercise of religion create a correlative freedom of association: a right to remain free from public regulation affecting expressive or religious activity.

The state action doctrine directly parses the public-private line. State action is subject to constitutional restrictions; constitutional rights protect non-state action. Since the Industrial and Jacksonian revolutions, collective economic activity has generally been viewed as non-state action, unless directly undertaken by the state.¹⁹⁰ (This was not always the case.)¹⁹¹ The Progressive Era and New Deal did not seem to redraw the line between public and private: neither corporatism nor socialism ever took deep root. However, the regulatory state changed the relationship between the public and private sectors, as the public sector played an increasingly intrusive role in governing the private sector. The 1960s almost heralded a major change, with courts increasingly finding state action in

187. It also constrains otherwise-private actors “acting under color” of law. 42 U.S.C. § 1983 (Supp. IV 1998). *See, e.g.,* Wyatt v. Cole, 504 U.S. 158 (1992) (liability for private persons who took advantage of unconstitutional replevin statute).

188. Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. Rev. 543, 580-86 (2000).

189. *But see* American Trucking Ass'ns, Inc. v. EPA, 175 F.3d 1027, 1034 (D.C. Cir. 1999) (per curiam), *modified on reh'g*, 195 F.3d 4 (D.C. Cir. 1999), *cert. granted*, 120 S. Ct. 2003 (May 22, 2000) (possible revival of old doctrine?).

190. *See, e.g.,* STANLEY KUTLER, PRIVILEGE AND CREATIVE DESTRUCTION: THE CHARLES RIVER BRIDGE CASE (1971); RONALD E. SEAVOY, THE ORIGINS OF THE AMERICAN BUSINESS CORPORATION: 1784-1855 (1982); Santa Clara County v. Southern Pac. R.R. Co., 118 U.S. 394, 396 (1886).

191. In the late eighteenth century, all collective economic activity was commonly viewed as belonging to the public sector, and the legitimacy of non-statal collective economic activity was in doubt. *See* HORWITZ, *supra* note 5, at 111-14; FRANK BOURGIN, THE GREAT CHALLENGE: THE MYTH OF LAISSEZ-FAIRE IN THE EARLY REPUBLIC (1989) (economic role of the state). I have argued that this extends beyond the corporate form, to large-scale economic activity in general. Joseph H. Sommer, *The Birth of the American Business Corporation: Of Banks, Governance and Social Responsibility* (2000) (unpublished manuscript, on file with author).

previously sacrosanct private economic activities.¹⁹² For almost all economic activities, this trend abruptly reversed in the 1970s.¹⁹³ Today's state action doctrine places most economic actors firmly on the private side of the fence.¹⁹⁴

There is no reason to believe that the courts will treat the Internet any differently.¹⁹⁵ Contemporary constitutional law has no problem viewing the New York Stock Exchange and the National Association of Securities Dealers as "private" organizations, albeit heavily-regulated ones.¹⁹⁶ These organizations not only have the power to deprive members of their livelihood, they may also fine them and expect their fines to be enforced by a court. If *these* organizations are "private," the Internet will surely withstand the state action doctrine, barring a constitutional revolution.

Antitrust law more plausibly regulates Internet governance. Antitrust law works only on actors who are private in the state action sense. However, antitrust is a narrow tool. Antitrust may resemble review of public-sector action if the private regulation is imposed in statal fashion, for example, a trade organization imposing rules and sanctions on its members. In such cases, courts have not been very sympathetic to the trade organization, especially if the rules affect members' conduct toward nonmembers.¹⁹⁷ But antitrust is somewhat less aggressive when the rules are im-

192. See, e.g., *Burton v. Wilmington Parking Auth.*, 365 U.S. 715 (1961); *Silver v. NYSE*, 373 U.S. 341 (1963) (antitrust case); *Amalgamated Food Employees Union v. Logan Valley Plaza*, 391 U.S. 308 (1968), *overruled by* *Hudgens v. NLRB*, 424 U.S. 507 (1975); *Fuentes v. Shevin*, 407 U.S. 67 (1972).

193. See, e.g., *Jackson v. Metro. Edison Co.*, 419 U.S. 345 (1974); *Hudgens v. NLRB*, 424 U.S. 507 (1975); *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972); *United States v. NASD*, 422 U.S. 694 (1975); *Flagg Bros. v. Brooks*, 436 U.S. 149 (1978); see also Gary D. Spivey, Annotation, *Validity, Under Federal Constitution and Law of Self Help Repossession Provision of § 9-503 of Uniform Commercial Code*, 29 A.L.R. Fed. 418 (1976). *But see* *Lugar v. Edmonson Oil Co.*, 457 U.S. 922 (1982).

194. There are some exceptions. E.g., *Lebron v. Nat'l R.R. Pass. Corp.*, 513 U.S. 374 (1996); *Goodyear Atomic Corp. v. Miller*, 486 U.S. 174 (1988); *Boyle v. United Tech. Corp.*, 487 U.S. 500 (1988). It should be noted, however, that the latter two cases benefited the economic actor.

195. See Berman, *supra* note 171.

196. The case law for exchanges mirrored the general revolution in the public-private sector marked by *Metropolitan Edison*. Compare *Intercontinental Indus. v. Am. Stock Exch.*, 452 F.2d 935 (5th Cir. 1971) (American Stock Exchange state actor), with *United States v. Solomon*, 509 F.2d 863 (2d Cir. 1975) (citing *Metropolitan Edison*); *First Jersey Sec. v. Bergen*, 605 F.2d 690, 698 & 699 n.5 (3d Cir. 1977); *Desiderio v. NASD*, 191 F.3d 198, 206 (2d Cir. 1999).

197. E.g., *Fashion Originator's Guild v. FTC*, 312 U.S. 457 (1941); *Associated Press v. United States*, 326 U.S. 1 (1945); *Silver*, 373 U.S. at 341. *But see, e.g.*, *SCFC ILC, Inc. v. VISA USA, Inc.*, 36 F.3d 958 (10th Cir. 1994).

posed as code, through some kind of multilateral standard-setting context, such as credit card association operating rules. (Unilateral imposition of standards is even more difficult to regulate with antitrust tools.)¹⁹⁸ The test for antitrust liability in standard setting is narrow. Absent gross procedural unfairness or a demonstration that the competitive harm imposed by the standard exceeds its benefits,¹⁹⁹ the courts will defer to private standards. The harm is almost always defined in narrow consumer-welfare terms, although the benefit might be viewed more broadly.²⁰⁰ Therefore, antitrust law—apart from restricting some state-style regulations—should not be expected to have a major influence on Internet governance.

The First Amendment creates two public-private distinctions. One is a modified version of the state actor distinction. The First Amendment's state actor distinction generally tracks the case law discussed above, but also serves to regulate the state's formulation of private law.²⁰¹ The other public-private distinction of the First Amendment applies only to private parties. Some expressive activity is so inviolably private that the state cannot regulate it, such as freedom of association. Other expressive activity is more amenable to regulation.²⁰² First Amendment state action and freedom of association are significant constraints on the Internet. If particular devices—such as “filters” that block browser access to objectionable content—implicate freedom of association, they cannot be regulated. If they are state action, they are probably unconstitutional. Only if they are in between are they regulable.

In conclusion, the public-private divide in cyberspace is a rich and interesting topic. However, it is most interesting where the legal constraints

198. See Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041, 1067-80 (1996); cf. *United States v. Microsoft*, 84 F. Supp. 2d 9 (D.D.C. 2000) (finding of facts); 87 F. Supp. 2d 30 (D.D.C. 2000) (denying declaratory judgment and dismissing counterclaim); 97 F. Supp. 2d 59 (D.D.C. 2000) (antitrust liability for unilateral imposition of standards).

199. E.g., *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988); *Am. Soc'y of Mech. Engineers v. Hydrolevel Corp.*, 456 U.S. 556 (1982) (cases stress fair procedures).

200. See *United States v. Brown Univ.*, 5 F.3d 658 (3d Cir. 1993).

201. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), was a conventional state-action case, because it was restricted to public officials in their official capacity. Soon, the *N.Y. Times* case was expanded to public figures. See *Curtis Publ'g Co. v. Butts*, 388 U.S. 130 (1967). With *Curtis Publishing*, the Supreme Court created another constitutional mystery akin to *Shelley v. Kraemer*, 334 U.S. 1 (1948).

202. Compare *Boy Scouts of Am. v. Dale*, 120 S.Ct. 2446 (2000) (latest freedom-of-association case), with *Robins v. PruneYard Shopping Ctr.*, 447 U.S. 74 (1980) (a shopping center, although not a state actor, is not so private that state cannot regulate speech there).

are least visible. The public-private divide has little legal bite on the Internet, outside of First Amendment law and a few extreme antitrust cases.

B. Choice-of-Law in Banking—An Historical Romance

Electronic banking predates the Internet by over a century and a half.²⁰³ Given this long history, new problems of cyberlaw may be very old issues in banking law. Choice-of-law is a good example. Much of the recent “cyberlaw” literature has hinted that current law is inadequate to meet the challenges of a borderless medium.²⁰⁴ This assertion is no longer true for choice-of-law in international banking. Mid-twentieth-century choice-of-law theory was ill-suited to the challenges of modern telecommunications. The law had to change, and change it did. In the late 1980s and throughout the 1990s, international banking law has been transformed.²⁰⁵ However, the new telecommunications-friendly law was adopted wholesale from nineteenth and early twentieth-century legal principles and doctrines. This ancient law had been trashed in mid-century by legal realism, only to be revived at the end of the century when demanded by an increasingly electronic and international banking practice. In cyberspace, the old ways are sometimes the best ways.

The history of this field of law is almost novelistic. Our hero, choice-of-law in banking, begins life as a naïf, but with excellent parentage.²⁰⁶ After a tranquil childhood, our hero has a great adventure—the Russian Revolution. Although our hero falls into peril during the Revolution,²⁰⁷ our hero emerges with experience and wisdom.²⁰⁸ At this point, our *bildungsroman* becomes a bastard mix of Gothic and Harlequin romance. The early UCC had a chance to befriend banking choice-of-law, but ig-

203. See *supra* note 7 and accompanying text; *supra* note 151; *supra* text accompanying note 161.

204. See Goldsmith, *supra* note 40 (describing and debunking jurisdictional claims of “regulation skeptics” that conventional legal principles are inapplicable to the Internet).

205. See Sommer, *supra* note 100, at 1191-92.

206. One cannot do much better than Justice Story. See *Bank of the United States v. Goddard*, 2 F. Cas. 694, 696 (C.C.D. Mass. 1829) (No. 917). This may be the first case that discussed the liability of the same bank in multiple jurisdictions.

207. The extensive citation history of the great *Sokoloff* case alone reads like the perils of Pauline. *Sokoloff v. Nat'l City Bank*, 196 N.Y.S. 364 (Sup. Ct.), 199 N.Y.S. 355 (Sup. Ct. 1922), *rev'd*, 204 N.Y.S. 69, 949 (App. Div. 1924), *aff'd*, 145 N.E. 917, *re-manded*, 224 N.Y.S. 102 (N.Y. Sup. Ct. 1927), *aff'd without op.*, 227 N.Y.S. 907 (App. Div. 1928), *aff'd*, 164 N.E. 745 (1928).

208. *M. Salimoff & Co. v. Standard Oil Co.*, 186 N.E. 679 (N.Y. 1933) (overruling Judge Cardozo's opinion in *Sokoloff*); *Bluebird Undergarment Corp. v. Gomez*, 249 N.Y.S. 319, 323 (City Ct. 1931); *Dougherty v. Nat'l City Bank*, 285 N.Y.S. 491, 505 (Sup. Ct. 1935).

nored the opportunity.²⁰⁹ Banking choice-of-law, with no strong statutory friend, was seduced by the villains of the piece—the *Restatement (Second) of Conflicts of Law* and contemporary choice-of-law theory. Case by case, our hero slowly becomes mad.²¹⁰ But all's well that ends well and in the 1980s, the UCC marries the conflicts law of banking.

The story has been told before,²¹¹ but can bear a brief retelling. Even in the prewar era, banks were multinational enterprises. The leading banks often had branches around the world. Their main product—the bank account—was a pure promise with no physical existence.²¹² The bank promisor—a multinational—had no unique location. Often enough, the promisee—the depositor—was also disperse. Such a promise can be as intangible and pervasive as the luminiferous ether—or the Internet. However, the lawyers of old could handle the challenge. They appreciated the proper legal technique: formalism.

The conflict of laws theory of the late nineteenth and early twentieth centuries was extremely formalistic, associated with names like Beale and Story.²¹³ Given this formalism, prewar banking law had no problems associating each promise with a unique branch. The guiding trope was physical—the promised clink of gold over the branch's counters. A bank account, therefore, was governed by the law of the place in which the bank promised to pay the gold (or later, the currency.) No matter that gold or currency were seldom used as a bank payment medium; formalism does not care about reality. No matter where the depositor wrote and delivered the checks; formalism takes no heed of facts it deems irrelevant. Bank ac-

209. U.C.C. § 1-105 (1999) did little to formulate conflicts rules, except to recognize party autonomy. In the 1962 text, the only banking conflicts rules were found in UCC §§ 4-102(2), 4-106 (1999).

210. The madness was progressive: running from illogic to denial, and culminating in stark legal lunacy. See *J. Zeevi & Sons, Ltd. v. Grindlays Bank (Uganda) Ltd.*, 333 N.E.2d 168, 172-73 (N.Y. 1975) (analysis hinging on non sequitur); *Vishipco Line v. Chase Manhattan Bank, N.A.*, 660 F.2d 854, 863-64 (2d Cir. 1981) (appellate court ignored inconvenient findings of trial court); *infra* note 223 (distinguished appellate courts cannot agree on identical facts). *Zeevi* is discussed in Sommer, *supra* note 66, at 47-53; *Vishipco* is discussed in Sommer, *supra* note 66, at 44 n.135.

211. Jefferson B. Fordham, *Branch Banks as Separate Entities*, 31 COLUM. L. REV. 975 (1931), Patrick Heining, *Liability of U.S. Banks for Deposits Placed in Their Foreign Branches*, 11 LAW & POL'Y INT'L BUS. 903 (1979); Richard Herring & Friedrich Kübler, *The Allocation of Risks in Cross-Border Deposits*, 89 NW. U. L. REV. 942 (1995); Sommer, *supra* note 66.

212. This point is made repeatedly in Sommer, *supra* note 66.

213. See JOSEPH H. BEALE, A TREATISE ON THE CONFLICT OF LAWS (1935); JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS (1st ed. 1834).

counts were governed by the law of an arbitrary jurisdiction specified by the parties and that worked well enough.²¹⁴

Formalism works well for the law of banking because there is nothing for realism to grip. As discussed above, nineteenth-century banking evolved from a trade in gold to a trade in accounts.²¹⁵ Payment of an account is not a physical act but a symbolic one—transforming a credit at X's account to a corresponding credit at Y's account.²¹⁶ There is nothing "real" in this transformation, just performative utterances. Formalism operates on facts, transforms them into a categorical pattern, and maps this categorical pattern onto a legal result through legal doctrine. Facts are messy, and the neatness of the patterns belies a difficult fitting process. However, if the relevant facts are symbolic in nature, the transformation is trivial. Symbols are not messy: the symbols are the facts are the pattern.²¹⁷ The result is a very satisfactory kind of super-formalism, which I have called "legal nominalism."²¹⁸ Payment law is an utterly pure law of symbols, in which the only disputable facts relate to the authenticity and integrity of records, and the authority of the authenticator.

Substantive payment law has always been formalistic. The old adjective law was also formalistic and therefore could easily ascribe a location to these utterances.²¹⁹ The old formalistic choice-of-law rule applied the law of the branch in which the account was "kept," or the account was "payable."²²⁰ True, the account was rarely "paid" by corporeal means. There was seldom a clink of gold or even a rustle of banknotes, just debits and credits on paper. But the old formalistic courts did not care about this. They looked to what was written on an account agreement or instrument.

This approach could not long survive legal realism. The legal realists of the 1920s and 1930s asserted that the emperor had no clothes and courts

214. Sommer, *supra* note 100, at 1186-88.

215. See *supra* text accompanying notes 92-94.

216. Even modern legal doctrine pretends that this is not the case—that payment of money has something to do with a right to currency. Cf. U.C.C. § 1-201(24) (1999); Geva, *supra* note 93. However, the law drops this fiction whenever it has to deal with real problems. See U.C.C. § 4A-406(b) (1989) (wire transfer discharges obligations except under extraordinary circumstances); Sommer, *supra* note 66, at 17 n.42 (collecting citations to courts ignoring inappropriate monetary legal fictions).

217. See Sommer, *supra* note 66, at 60-61; Frederick Schauer, *Formalism*, 97 *YALE L.J.* 509 (1988).

218. See Sommer, *supra* note 66, at 60-64.

219. See Sommer, *supra* note 100, at 1187.

220. See Sommer, *supra* note 66, at 66-73.

should only look to the underlying reality of the transaction.²²¹ Realism is generally a useful thing, but what if there is no underlying reality—what if clothes make the emperor? The confident formalism of the old law created the feeling that bank accounts had a location, just like the confident formalism of banking law creates the feeling of money, which is money itself. When realist courts realized that modern telecommunications made geography irrelevant and stripped the territorial formalism away, little remained. The courts of the 1970s and 1980s correctly realized that an account location was anywhere a court deemed it to be.²²²

Bankers and their regulators were unhappy with this state of affairs.²²³ The result was a wave of statutory codification in the late 1980s and early 1990s. Most of these statutory changes were in the UCC,²²⁴ but some regulatory statutes also reflected these changes.²²⁵ The bankers' new law resembled the old formalistic law. It assumed that bank accounts had a location, and this location was determined by stereotyped communications of the parties, not by any realities of the transaction. UCC Articles 8 and 9 take formalism one step further into explicit nominalism. Both statutes construct a hierarchy of symbols that indicate governing law.²²⁶

This law also made clear that if a bank assumes multiple roles, each role can be governed by a separate law. For example, an agreement that calls for a bank to honor a letter of credit in one country and pay in another calls for separate legal systems controlling honor and payment.²²⁷

221. See LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 688-89 (2d ed. 1985).

222. The first commentator to articulate this was Margaret E. Tahyar, Note, *The Act of State Doctrine: Resolving Debt Situs Confusion*, 86 COLUM. L. REV. 594 (1986). An early decision that understood the irrelevance of geography was *Digitrex, Inc. v. Johnson*, 491 F. Supp. 66 (S.D.N.Y. 1980).

223. If there were no reality constraining the court's will, Wednesday's opinion could favor one side, and Friday's opinion the other, with identical facts. This sounds hyperbolic; it is not. Distinguished appellate courts issued these very opinions on exactly these days in the same week in 1984. Compare *Garcia v. Chase Manhattan Bank*, 735 F.2d 645 (2d Cir. 1984) (plaintiff wins on Wednesday), with *Perez v. Chase Manhattan Bank*, 463 N.E.2d 5 (N.Y. 1984) (on Friday of the same week, plaintiff loses with the same facts). The unhappy reaction of banks and their regulators can be found in various amicus briefs. See Sommer, *supra* note 66, at 49 n.156.

224. See U.C.C. § 4-102(b) (1999); U.C.C. § 4A-507 (1989); U.C.C. § 5-116(b); U.C.C. § 8-110 (1999); U.C.C. § 9-304 (2000).

225. See 12 U.S.C. § 633 (1994); N.Y. BANKING LAW § 138 (McKinney 1990).

226. U.C.C. § 8-110(e) (1999) (securities intermediaries); U.C.C. § 9-304(b) (2000) (banks); U.C.C. § 9-305(b) (2000) (commodities intermediaries).

227. *Chuidian v. Philippine Nat'l Bank*, 976 F.2d 561 (9th Cir. 1992); cf. *Canadian Imperial Bank of Commerce v. Pamukbank Tas*, 632 N.Y.S.2d 918 (Sup. Ct. 1994) (hold-

This discussion shows that some aspects of conflicts law become *simpler* in cyberspace. Tangible facts—the relevant locations of people, organizations, or things—can often be more complex than virtual ones. If we can limit ourselves to these virtual facts of cyberspace—the symbolic content of communications—we may have a virtual law: elegant and tractable.

C. Jurisdiction

We now turn from choice-of-law to jurisdiction. We discuss jurisdiction in two contexts: personal jurisdiction, and jurisdiction to prescribe or regulate.

1. Personal Jurisdiction

There is nothing either elegant or tractable about the U.S. law of personal jurisdiction. This is not a statement of necessity. It is possible to draft a relatively simple and useful statute regulating judicial jurisdiction—the draft Hague Convention is good evidence of this.²²⁸ However, our current law of jurisdiction touches on some of our deepest legal emotions, and is a product of contingency rather than design. It keeps evolving by pure historical logic: accretion on accretion, resistant to any discernable underlying policy.

Cyberspace does not affect the difficulty of U.S. jurisdictional law. Modern telecommunications technology may have increased the salience of its problems, but they have been bad enough for a long time.²²⁹ Much of the discussion of the jurisdictional law of cyberspace is therefore misplaced. It is a difficult field of law, but the difficulties lie with the fundamental law of jurisdiction. Any additional difficulties posed by modern information technology are a small wrinkle on an already serious problem.

Interstate personal jurisdiction over corporations is a good place to start, because it encapsulates the problems of U.S. jurisdictional law.²³⁰ Since most states' long-arm statutes reach to their constitutional limits, the usual U.S. law of jurisdiction is constitutional law. Jurisdiction, then, is

ing bank—whose role as letter of credit issuer was governed by Turkish law—was governed by New York law in its obligation to reimburse Canadian confirmer).

228. Preliminary Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters (adopted 30 October, 1999), <http://www.hcch.net/e/conventions/draft36e.html>.

229. This is precisely the point made by Professor Redish, *supra* note 154. I have bothered to develop an independent analysis only because we have different notions of what should be the law of jurisdiction.

230. For a far more thorough discussion of these issues, including references to foreign law, see *ABA Report*, *supra* note 154, ch. 3.

limited only by the Due Process Clause, which requires "minimum contacts" to assure constitutional "fair play and substantial justice."²³¹ The two standards must be independently met, but appear to overlap in the usual case.²³²

The terms "minimum contacts" and "fair play and substantial justice" are scarcely self-defining. "Fair play and substantial justice" is particularly useless. Any legitimate legal rule, regardless of its content, would seem to advance this vague standard. "Minimum contacts" is somewhat less otiose. It implies that some jurisdictions might have too attenuated a connection with a particular dispute, but does not seek to discriminate between the marginally adequate and more appropriate jurisdictions.

Neither of these terms comes close to answering the real question: why do we want any limits on a court's personal jurisdiction? Jurisdictional doctrine carefully avoids the obvious answer: regulation of forum shopping. Indeed, the Supreme Court has appeared to relegate this task to the shadowy forum non conveniens doctrine, acknowledging that jurisdiction has little meaningful role to play.²³³ The law of jurisdiction is in dire need of a rationale that is neither vague nor self-referential.

Without changing the underlying policies (if any exist), the Supreme Court has continued trying to refine the doctrine. The attempt at definition has produced tests such as the "purposeful availment" test of *World-Wide Volkswagen*,²³⁴ and the "focal point" analysis of *Calder v. Jones*.²³⁵ *Calder*—limited to intentional torts such as libel—teaches that jurisdiction exists if the defendant intended to harm the plaintiff in the forum state.

"Purposeful availment" means that a defendant who has "purposefully" obtained benefit from commerce in other jurisdictions may "reasonably anticipate being haled into court there."²³⁶ The key word is "purposefully." The damages may have been foreseeable, but if the defendant's operations did not somehow reach out to another state, the harm is not "purposeful." This implies some kind of passive-active distinction: an intuitively appealing but analytically tricky delineation. A burger stand or

231. *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 320 (1945).

232. *Burger King v. Rudzewicz*, 471 U.S. 462, 476-77 (1985) (standards independent); *Asahi Metal Industry Co. v. Superior Court*, 480 U.S. 102, 116 (1987) (standards would diverge only in "rare cases" such as the one at bar).

233. *Piper Aircraft Co. v. Reyno*, 454 U.S. 246, 250-52 (1981).

234. *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980); *Calder v. Jones*, 465 U.S. 783 (1984).

235. *Calder*, 465 U.S. 783.

236. In other words, the defendant has "fair warning" that it may be "subject to the jurisdiction of a foreign sovereign." See *Shaffer v. Heitner*, 433 U.S. 186, 216 (1977).

auto dealership cannot be sued in tort outside its home state. (Matters are different in contract.)²³⁷ But if the out-of-state consequences of a defendant's actions are not sufficiently passive—a decision made by a multipart balancing test (*Asahi Metal*)²³⁸—a court may find purposeful availment, and will entertain a tort suit. The elements in such a test may include factors such as: “designing the product for the market in the forum State, advertising in the forum State, establishing channels for providing regular advice to customers in the forum States, or marketing the product through a distributor who has agreed to serve as the sales agent in the forum State.”²³⁹ This inquiry is contextual: no “talismanic jurisdictional formulas” exist.²⁴⁰ In other words, there is no jurisdictional predictability.

The result is something that resembles common law decisionmaking gone wild: a few oases of disconnected predictability, not linked by any broadly accepted theoretical or doctrinal understanding. In between, all is indeterminate, although with a tilt toward the clever forum-shopper. To make matters worse, it is a matter of federal constitutional law. No fact pattern is settled until the Supreme Court chooses to speak, and new fact patterns always emerge.

Given this mess, it is hard to see how cyberspace will make things better—or worse. The Internet will doubtless contain its own oases of predictability, as disconnected as all others. In cyberspace, how does one know that one is availing oneself of a forum?²⁴¹ Is posting a website active or passive? If passive, what more is required? Who knows? The case law will eventually tell us. Either answer would doubtless be consistent with “fair play and substantial justice.”

2. *Jurisdiction to Prescribe*

The U.S. Constitution places few limits on the legislative jurisdiction to prescribe. If Congress may regulate any conduct, it may regulate that conduct by any person, anywhere, subject only to some mitigating rules of construction.²⁴² Fortunately, Congress and its regulators have exercised some modesty and definite jurisdictional limits may be discerned. For example, a foreign brokerage may sell foreign securities to foreign custom-

237. *Burger King*, 471 U.S. at 462.

238. *Asahi Metal Industry*, 480 U.S. at 112.

239. *Id.*

240. *Burger King*, 471 U.S. at 485.

241. See Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J. L. & TECH. 3, ¶¶ 44-46 (1997).

242. See *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) (statutes construed against violating rules of international law, if possible, otherwise enforced).

ers, without any fear of an SEC enforcement action.²⁴³ Under some circumstances, it may even sell these securities to U.S. citizens.²⁴⁴

These limits are not constraints on the power of Congress; they are merely useful prudential rules of thumb. The Internet does not seem to have changed them much, although it is placing more emphasis on “targeting” as a jurisdictional factor.²⁴⁵ Congress or its regulators will often assert extraterritorial economic jurisdiction over those who target U.S. persons, particularly consumers. Targeting is conceptually similar to the “purposeful availment” test of personal jurisdiction: a matter of intent more than deed. As with “purposeful availment,” one cannot infer targeting from a few adventitious customers. However, conduct directed toward acquiring these customers may be deemed an attempt to target such customers, even if the attempt does not succeed. Although targeting resembles “purposeful availment,” it can have the great advantage of clarity. Targeting may be defined by administrative implementation through detailed prospective rules, rather than fuzzy multi-part standards applied retrospectively in litigation.

Targeting is well-suited to the Internet. The only physical location it views as relevant is the one of the person (usually a natural person) receiving regulatory solicitude. Most individuals live in a unique physical location, notwithstanding the jet plane and the Internet. However, targeting is an old jurisdictional factor, perfected in particular by the SEC.²⁴⁶ To be sure, the Internet makes some difference. Internet advertisements are available in all jurisdictions, unlike most conventional advertising media. (Some newspapers or magazines, such as *The Economist*, *The International Herald-Tribune*, are as jurisdictionally ubiquitous as the Internet.) Fortunately, the novel challenges of the Internet appear interstitial and soluble, although an optimal solution will doubtless require some experimentation. For example, one tentative solution of the SEC absolves offerors of nonregistered foreign offerings from U.S. liability if their websites contain “reasonable measures” to discourage U.S. participation in foreign offerings, such as disclaimers or identification checks.²⁴⁷

243. See *infra* note 246.

244. See *id.*

245. ABA Report, *supra* note 154, § 2.2.

246. See, e.g., 17 C.F.R. §§ 230.902(b) (2000) (directed selling of restricted securities in the United States); *id.* § 240.15a-6 (foreign broker-dealer registration).

247. 63 Fed. Reg. 14,806 (Mar. 27, 1998).

D. Enforcement and International Cooperation

We abandon judicial jurisdiction as a hopeless mess, with or without the Internet. We also abandon jurisdiction to prescribe, which seems to involve little in the way of novelty. We now turn to enforcement of judgments and other forms of international legal cooperation. As Professor Coffee points out, enforcement and international cooperation are much more complex issues than jurisdiction.²⁴⁸ Assertion of jurisdiction is unilateral, constrained by nothing outside the court or legislature that does the asserting. But enforcement of foreign judgments and other forms of cooperation are not unilateral. Cooperation, therefore, is more complex than jurisdiction, requiring shared conduct, some shared assumptions, and perhaps shared discourse.

Not only is cooperation more difficult, it may be more important than the law of jurisdiction. The worst that can be said about the law of personal jurisdiction is that it is a conceptual muddle that permits an excessive degree of forum shopping. Forum shopping (or its congener, multiple liability) can be lethal in those fields of law that call for extreme precision, especially when conjoined with imprecise conflicts rules.²⁴⁹ However, some degree of forum shopping is probably a tolerable evil in general law, especially because the law of enforcement serves as a safety valve on some of its worst excesses.²⁵⁰ The worst that can be said about the law of prescriptive jurisdiction is that simultaneous compliance with several jurisdictions' rules is difficult. On the other hand, few jurisdictions have flatly contradictory rules, and the added lawyers' fees are a cost of doing business. As we shall see, however, an unsatisfactory law of enforcement—or unsatisfactory international legal cooperation—has serious implications for the international order.

International legal cooperation has several dimensions, of which enforcement of civil judgments is only one. Other dimensions consist of international aid in fact-finding and extradition. Sovereigns do not always cooperate in these endeavors for several reasons. Courts have traditionally refused to enforce penal or tax judgments, or judgments contrary to local

248. Cf. John C. Coffee, Jr., *Brave New World?: The Impact(s) of the Internet on Modern Securities Regulation*, 52 *BUS. LAW.* 1195, 1227-29 (1997). Professor Coffee's observation was limited to securities law, but easily generalizes to libel, obscenity, Internet gambling, and the like.

249. This is particularly the case in banking law. Sommer, *supra* note 100, at 1204-09.

250. Goldsmith, *supra* note 40, at 1216-19.

public policy.²⁵¹ As a result, a person whose assets exist only in the United States may have remarkable worldwide freedom of libel by world standards.²⁵² A securities broker whose assets are in a jurisdiction that extols insider trading might enjoy similar protections from the grasp of United States securities law. Extradition is traditionally a matter of grace, absent a treaty, and requires double criminality even with a treaty. Many forms of information will not easily pass international borders, especially in public law.²⁵³

Most of these limitations on international cooperation are traditional, interstitial, and tolerable. The norm has been a reasonable comity. However, with an increasingly globalized economy, this norm has been under strain in recent decades. The strains on comity are being addressed by measures such as the draft Hague Convention,²⁵⁴ which hopes to enhance enforcement of foreign judgments in exchange for shrinking the jurisdictional bases upon which these judgments were obtained. This story is basically one of globalization, and is older than the Internet. However, the Internet has some real roles, albeit secondary ones. We study two of them here.

1. Case Study: Secrecy Jurisdictions

A number of postwar sovereigns possess an odd collection of attributes: small size, low sovereign risk, reasonably sophisticated commercial law, and few visible means of support. This combination of attributes has proven surprisingly profitable. These sovereigns have withdrawn from many ordinary forms of international legal cooperation. Instead, they have used their local law to lubricate the wheels of illicit commerce; the illicitness defined or adjudicated elsewhere. Their small size and few other means of support make them resistant to retaliation; their sophisticated commercial law and low sovereign risk make them very user-friendly.²⁵⁵

251. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 482(2)(d), 483 (1987).

252. See *Matusevitch v. Telnikoff*, 877 F.Supp. 1 (D.D.C. 1995), *aff'd*, 702 A.2d 230 (Md. 1997), *aff'd without published op.*, 159 F.3d 636 (D.C. Cir. 1998) (English libel judgment not enforceable in Maryland, because England's law of libel contrary to Maryland public policy).

253. See RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 432 reporter's note 1 (1987).

254. See Preliminary Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters (adopted 30 October, 1999), <http://www.hcch.net/e/conventions/draft36e.html>.

255. Many of these ideas are developed by Stewart F. Sterk, *Asset Protection Trusts: Trust Law's Race to the Bottom*, 85 CORNELL L. REV. 1035 (2000).

These jurisdictions are often known as “secrecy jurisdictions,” so-called because bank secrecy laws might have been the first of this genre.²⁵⁶ Bank secrecy laws allow such a jurisdiction to harbor or hide offshore assets by hiding the identity of the owner. Secrecy is not the only possible approach. By means of bald judgment-proofing, a trust can protect or conceal assets without even concealing the identity of the beneficiary. In secrecy jurisdictions, trusts are often revocable at the will of the grantor-beneficiary, but are nonetheless impregnable to legal attack.²⁵⁷

“Secrecy jurisdiction” is a pejorative term, and many jurisdictions impose substantial limitations on international cooperation.²⁵⁸ Pejorative distinctions are inappropriate, unless there is a reason for them. The reason for distinguishing secrecy jurisdictions from others does not so much lie in the content of their laws, but rather in the incentives of the jurisdictions. Ordinary jurisdictions are constrained by reciprocity; secrecy jurisdictions are not. Therefore, ordinary jurisdictions will tend to cooperate except when cooperation would violate a strong local norm. Secrecy jurisdictions instead profit from noncooperation. We therefore expect to see the scope of secrecy jurisdiction protections continue to expand to their technological limits.

Secrecy jurisdictions predated the Internet, and the story of secrecy jurisdictions is primarily a story of globalization. However, the Internet has aided these jurisdictions in providing their services to the mass market. Before the Internet, international enforcement limitations and secrecy jurisdictions were the playground of large-scale business, such as money laundry, or at least the carriage trade, such as tax avoiders or judgment proofers. Before the Internet, a retail business had a hard time keeping its assets in one jurisdiction and its customers in another. But now, one can gamble or bank on the Internet with a Caribbean financial institution from the comfort (if not safety) of one’s home. One can trade securities using an unregistered foreign broker or download exotic foreign graphics, for that matter.

256. Switzerland may have been the first of the bank secrecy jurisdictions. It is not typical of today’s secrecy jurisdictions, because Switzerland has a substantial domestic economy, and is a power in several world markets. It is worth noting, however, that Switzerland no longer provides the kinds of unusual legal protections to the illicit offshore business of foreign customers that would get it on the lists discussed *infra* note 259 and accompanying text.

257. See Sterk, *supra* note 255.

258. See, e.g., RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 479 (1987) (describing limitations on Hague Convention).

Nonsecrecy jurisdictions cannot use their traditional legal means—comity extended in private international law—for controlling the conduct of secrecy jurisdictions. At least three general approaches remain. First, the nonsecrecy jurisdictions could provide secrecy jurisdictions with non-judicial incentives for cooperation, either carrots (e.g., foreign aid) or sticks. This is often difficult, requiring collective action on the part of the nonsecrecy jurisdictions. Nevertheless, it appears increasingly practicable.²⁵⁹ Second, the nonsecrecy jurisdictions could control their own citizens directly, restraining them from taking advantage of secrecy jurisdiction services. This is often difficult as a general matter, and might be particularly difficult—if perhaps not impossible—over the Internet.²⁶⁰

Finally, there is the prospect of “gatekeeper control”²⁶¹ imposing liability on an intermediary with local assets that has the ability to control the undesired offshore behavior. The vicarious liability implicit in gatekeeper strategies is quite popular in the “cyberlaw” literature,²⁶² but is very much old hat. Various telegraph cases in the earlier part of this century dealt with almost precisely the same subject.²⁶³

In principle, it may be difficult to impose effective gatekeeper control on the Internet, because there is no central authority that can vouch for the others, and because cryptography makes message control difficult. However, this principle might be less difficult in practice. First, most secrecy jurisdictions are in the business of fostering illegal commercial transac-

259. Such collective action appears to be mobilizing. The OECD, for example, has recently published a list of thirty-five jurisdictions that it deemed to be “tax havens.” See OECD Forum on Harmful Tax Practices, available at <http://www.oecd.org/media/release/taxnotes.htm> (last modified Mar. 3, 2000). The OECD is inviting these jurisdictions to eliminate their harmful practices. The OECD’s Financial Action Task Force on Money Laundering has released “Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures” (June 22, 2000), which identified fifteen jurisdictions as “non-cooperative.” See Financial Action Task Force on Money Laundering, <http://www.oecd.org/fatf/> (last visited July 24, 2000).

260. A jurisdiction, for example, may try to block secrecy jurisdictions with national firewalls. China, for instance, has tried this strategy. See Goldsmith, *supra* note 40, at 1227.

261. See Coffee, *supra* note 248, at 1202, 1229-30.

262. E.g., Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526 (1996); Hardy, *supra* note 154, at 1000-08; Goldsmith, *supra* note 40, at 1224-30; Perritt, *supra* note 154; 17 U.S.C. § 1201 (Supp. IV 1998) (imposing liability on those who develop technologies that aid infringement of copyright).

263. See, e.g., *Flynn v. Reinke*, 225 N.W. 742 (Wis. 1929); see also Smith, *supra* note 151.

tions. Commercial transactions generally require payment through the banking system, so gatekeeper control through banks may not be a chimera.²⁶⁴ Second, the retail level is usually intermediated through Internet service providers—established companies with assets in many jurisdictions. Gatekeeper control at this level may be quite practical.²⁶⁵

In conclusion, the Internet makes the services of secrecy jurisdictions available to the retail trade, and it makes effective cross-border regulation of secrecy jurisdictions somewhat more difficult. But apart from the retail issue, the Internet did not create any problems that had not existed before.

2. *Case Study: International Contract Formation and Public Key Infrastructure*

Part III argued that the common law of contract formation is so informal that it can easily accommodate electronic commerce with no stress. Apart from the knotty but limited issue of electronic agents, the even more limited issue of transferable records, and the consumer provisions of the Electronic Signatures in Global and National Commerce Act, there have been remarkably few novel legal developments in electronic contracting.

This argument, so far, is limited to U.S. law. Does it apply to foreign law as well? Most civil law countries have a much more formal law of contract formation than the United States. U.S. law permits a party to prove the contract using any admissible evidence (as usual, putting statute of frauds issues to the side). In contrast, many civil law countries require a notarial stamp: a trusted third party attestation of authenticity.²⁶⁶ Of course, there is an obvious electronic analogue to the notarial stamp: the public key infrastructure (“PKI”).²⁶⁷ A reliable PKI has the promise of providing excellent authentication and guarantees of message integrity, while preserving civil law legal traditions. Such an infrastructure may easily accommodate the notarial concept, especially if the infrastructure is regulated or otherwise semi-official. Within the borders of a civil law country, matters look much the same as within the United States. Modern electronic technologies pose no major problems, although civil law juris-

264. See *supra* note 156.

265. Goldsmith, *supra* note 40, at 1224-27. To be sure, gatekeeper control is impractical if encryption is taken for granted. However, I know of no technical reason why Internet service providers cannot control the encryption practices of their subscribers, if not their subscribers' counterparties.

266. THOMAS GLYN WATKIN, AN HISTORICAL INTRODUCTION TO MODERN CIVIL LAW 440-42 (1999).

267. For readers unfamiliar with PKI, see Froomkin, *supra* note 76; Winn, *supra* note 39.

dictions probably need implementing legislation and the United States does not.

However, electronic contract formation—although raising no serious legal problem within the borders of any country—may raise real cross-border problems. Civil law jurisdictions lean toward PKI; common law jurisdictions are experimenting with many structures.²⁶⁸ The PKI infrastructure may turn out to be unpopular in common law jurisdictions. PKI has its detractors who view it as fussy, expensive, impracticable, legally unstable, no more secure than private key, and harsh on unsophisticated users.²⁶⁹ These possible weaknesses of PKI raise the specter of a legal disconnect between an operationally flexible common law electronic commerce and a rigid civil law infrastructure. Common law jurisdictions will recognize PKI, but civil law jurisdictions might reject non-PKI methods. If the legal tail wags the business dog and the detractors of PKI are correct, the world might find itself saddled with an inferior operational system. If standardization proceeds on business lines (and the detractors of PKI are correct), many contracts might be unenforceable in civil law jurisdictions.

This obviously calls for a legal harmonization effort, a traditional task of the United Nations Commission on International Trade Law (UNCITRAL). UNCITRAL has already produced a first-round product: the 1996 Model Law of Electronic Commerce. This model law takes a UETA-style enabling approach, although its hard attribution rules are somewhat less friendly to unsophisticated parties in electronic commerce.²⁷⁰ This international harmonization effort is purely Internet-driven and of substantial legal and economic interest. However, as with the problem of retail and secrecy jurisdictions, it is part of a larger story, which is not an Internet story.

Harmonization is a major trend in postwar commercial law that has been accelerating over recent years.²⁷¹ Yet most of this harmonization is driven by globalization, not the Internet. Between 1958 and 1990, for example, UNCITRAL produced six model laws or conventions. Since then,

268. Compare Federal Act Establishing the General Conditions for Information and Communication Services, <http://www.iid.de/rahmen/iukdgc.html> (last visited Nov. 16, 2000) (Germany), with UNIF. ELEC. TRANSACTIONS ACT, prefatory note, §§ 5, 7, 7A U.L.A., 17-19, 28, 30 (Supp. 2000).

269. See Kaner, *supra* note 105; A. Michael Froomkin, *Article 2B as Legal Software for Electronic Contracting—Operating System or Trojan Horse?*, 13 BERKELEY TECH. L.J. 1023 (1998).

270. See *supra* note 63.

271. Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TUL. L. REV. 1931, 1936-40 (1998).

UNCITRAL has produced seven, with more on the way.²⁷² With the exception of the 1996 Model Law on Electronic Commerce, none of the 1990s lawmaking involved electronic commerce in any substantial way. Electronic commerce certainly requires international harmonization, but so does most everything else these days.

V. THE MISCELLANY

This section briefly discusses three common “cyberlaw” issues: privacy, intellectual property, and the First Amendment. These fields are at the core of much of the “cyberlaw” literature and I would feel remiss if I did not take at least a few wing shots at them. However, my interests are closer to the commercial law and sovereignty issues already discussed.

Privacy has been transformed by modern information technology in precisely the ways in which I have been skeptical in other contexts. However, the transformative agent was the mainframe computer of the 1950s, not the Internet, the personal computer, or any of the other recent informatics technologies.

The conclusion for intellectual property seems more complex. There are several very important—but very separate—stories here. One story—perhaps the most important one—resembles the privacy story. It is a story of a very significant technologically mediated transformation affecting the core, salience, and meaning of intellectual property law—involving very old information technologies. This story is that of the commodification of culture. Another story concerns a retreat from technology, namely the business-method patent. This story is generally outside the scope of this Article, but there is a point of tangency.²⁷³ Finally, there is the story of “digital rights management.” This story is technologically driven, and many of the relevant technologies are fairly new, although the Internet is probably not the most significant of them. The story is quite significant, although perhaps not as much as the commodification of culture. It may

272. Pre-1990: Convention on the Recognition and Enforcement of Arbitral Awards (1958), Limitation Period on International Sale of Goods (1974), Carriage of Goods by Sea (1978), Contracts for the International Sale of Goods (1980), International Commercial Arbitration (1985), International Bills of Exchange and International Promissory Notes (1988). Post-1990: Liability of Operators of Transport Terminals in International Trade (1992), Procurement of Goods and Construction (1992), International Credit Transfers (1992), Procurement of Goods, Construction and Services (1993), Independent Guarantees and Stand-By Letters of Credit (1995); UNCITRAL Model Law on Electronic Commerce (1997); Cross-Border Insolvency (1997). See United Nations Commission on International Trade Law, <http://www.uncitral.org> (last visited July 24, 2000).

273. See *infra* note 309.

therefore be the best cyberlaw story around. However, as we shall see, digital rights management straddles an old fault line in intellectual property law. These stories are not the only three, and the Internet contains some stories of its own. However, these other stories appear far less significant.

The First Amendment contains many stories, well-told in the contemporary literature. But I tell only a single cautionary tale.

A. Privacy

Privacy is a portmanteau concept, encompassing searches and seizures,²⁷⁴ public records, private records,²⁷⁵ the property rights of the famous in their fame,²⁷⁶ the rights of those who do not want to be famous,²⁷⁷ and the like. For our purposes, privacy does not include data security, which is limited to the commercial secrecy needs of commercial parties. We have already discussed data security, a traditional part of the law of records.²⁷⁸ Given the number of issues packed into the privacy portmanteau, any extensive legal treatment would be daunting, and a coherent conceptual treatment might be impossible. However, here we are only concerned with the effect of the new information technologies on the privacy nexus.

Privacy concerns have been around for a while. Privacy is vulnerable to any number of intrusive technologies, ranging from the policeman's crowbar to the printing press to the camera to the Internet. Electronic privacy became a legal issue with the wiretap case law of the 1920s.²⁷⁹ Electronic privacy took its modern form with the mainframe technology of the 1950s. This new technology facilitated several truly transformational social changes including the democratization and impersonalization of credit,²⁸⁰ the personalization of mass marketing, and the potentially enormous amounts of accessible information on individuals.

274. U.S. CONST. amend. IV.

275. See *Tournier v. Nat'l Provincial and Union Bank of Eng.*, 1 K.B. 461 (C.A. 1924) (confidentiality of bank records).

276. See *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977).

277. See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

278. See *supra* text accompanying notes 51-58.

279. See *Olmstead v. United States*, 277 U.S. 438 (1928).

280. Credit is no longer the ineffable (and personal) judgment of character sanctified by J.P. Morgan the elder. 3 DOCUMENTARY HISTORY OF CURRENCY AND BANKING IN THE UNITED STATES 231-33 (Herman Edward Krooss ed., 1983) (excerpts from 1913 Morgan'Pujo Report). Consumer credit has become a fairly objective number—almost a commodity.

It is easy to argue that this has created an enormous change in the meaning of personal privacy. With massive commercial databases, privacy is no longer a technological fact subject to primitive proprietarian notions. Personal information is no longer a "thing," over which one either exercises dominion or relinquishes control completely. To gain the benefits of democratized credit, we have surrendered our personal information to strangers: there are no secrets. However, we still hope to retain some control over the consequences of this surrender. Privacy as property has elided into privacy as license. Instead of secrecy, privacy now means "the power to control the facts about one's life."²⁸¹ Personal privacy has therefore become an exercise in trust—a social construct. Privacy law is consequently a legal ordering of social constructs: far more interesting and powerful than the more modest role of previous privacy law, which merely aided the primacy of physical dominion.

This argument has only one problem. It has little to do with the Internet, or with post-1970s informatics technology. The mainframe remains king of databases. Post-1970s technologies such as neural networks in data mining, the supermarket checkout scanner, or the Internet have only made a quantitative difference. Of course, the Internet now feeds the maw of the mainframe. But the banks already had much of the same information from credit card payments; the Internet merely makes it available to others. To be sure, the Internet has opened access to databases. But this makes little difference to privacy. The data implicated in commercial privacy are valuable, and are seldom given away for free on the Internet. Indeed, these data are so valuable that they were the subjects of markets even in the pre-Internet days.

Most adults have grown up with this entire system, along with its associated privacy concerns. Of course, the quantitative can shade into the qualitative, but the primary impact of the mainframe appears far greater than the secondary impact of more modern technologies. The incremental privacy erosion (or redefinition) of the last ten or fifteen years has been far less significant than that of the first thirty or forty years.

The Internet, however, may encourage a retrograde approach to privacy: a partial return to the old ways. Previous media were not inherently secure, but relied on trusted third parties such as banks, the post office and the telephone system.²⁸² On the Internet, all data strings are out in the

281. Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555 (1998).

282. This trust was enforced by law. See *Tournier v. Nat'l Provincial and Union Bank of Eng.*, 1 K.B. 461 (C.A. 1924); 62 C.J. *Telegraphs and Telephones* § 191 (1933).

open. This openness has stimulated the development of cryptanalytic secrecy.²⁸³ As a result, much of the Internet may be replacing our modern system of trust with old-fashioned secrecy, the arguable meaning of privacy before the mainframe. Internet privacy issues—mainly concerning the state's right or power to invade secrecy—seem more redolent of the old law than of the new.

B. Intellectual Property

Privacy has only one significant “law and technology” story: the mainframe. Intellectual property has several. But only one of these stories is both significant and related to new information technologies. We save this story—digital rights management—for the end, and discuss the others first.

1. *The Other Stories*

Perhaps the most important intellectual property story resembles the privacy story: a tale of legal and social transformation, enabled by technologies. The commodification of culture may be traced to the movies, if not before.²⁸⁴ For two examples, consider the community of trademark and the cult of celebrity.

Trademark—abetted by mass communication technologies—is becoming less a denotation of commercial quality than the commercial quality itself. A coffee mug bearing an NFL trademark is more valuable than a plain coffee mug, even if the mug manufacturer is the same. Ownership of such a mug denotes affiliation with a particular community, largely developed through television. This affiliation has psychic value to the mug owner. Thanks to trademark law, it has pecuniary value for those who control the symbols of the community. This implies a fascinating incentive to produce certain kinds of communities.

Celebrity always came with informal immunities; now it is associated with legal rights of intellectual property: the “right of publicity.”²⁸⁵ These rights help foster a commercially vibrant cult of celebrity. Of course, this tale is largely driven by technology, particularly the movies, television and music recording. The cult doubtlessly predated the technologies, and even some of the law: the names Jenny Lind, Edwin Booth and Lillian Russell still jog the memory. But de Tocqueville did not mention this cult: an in-

283. See Winn, *supra* note 44.

284. For an excellent description of the commodification of culture, see Rosemary J. Coombe, *Critical Cultural Legal Studies*, 10 YALE J.L. & HUMAN. 463, 464-69 (1998).

285. Sheldon W. Halpern, *The Right of Publicity: Maturation of an Individual Right Protecting the Associative Value of Personality*, 46 HASTINGS L.J. 853 (1995).

dication that it was marginal at one time. It no longer is, and is quite lucrative for its icons and their impresarios. The modern cult of celebrity raises some real concerns in a democratic polity.²⁸⁶

The commodification of culture is technologically driven in part, and may be the most important story involving intellectual property. It is not really a law-and-the-Internet story; rather it is a very typical one for a lawyer. Technology and law are both significant parts of this social story. Technology is a key enabler, but so is law reform. The story of recent copyright law reform is one of continuous expansion of the cultural industry: longer copyright terms and enhanced copyright protection of derivative works.²⁸⁷ Market forces drove both technology and law, notably the demands of the cultural industry. The Internet may further aid the commodification of culture, but the important technologies to date have been the mass media, particularly television, the movies, and the music technologies. Perhaps the Internet will be as important as any of these, but not so far. At least so far, the Internet's legal role resembles nothing so much as the Betamax's: a technology that happens to facilitate unauthorized copying.²⁸⁸

A few intellectual property issues are closely associated with the Internet. Most of them are not particularly significant. For example, consider the emerging property law in Internet addresses, aptly called "a species of mutant trademark," albeit one more consistent with a global economy.²⁸⁹ The law has some novelties, but the system of domain names is not novel. Telephone mnemonics (e.g., 1-800-SHYSTER) are structurally similar to domain names. These mnemonics are scarce informational resources, initially unallocated, but better allocated to certain parties than others. However, they have never received much legal notice, possibly because all numbers initially belonged to the telephone company, which had an incen-

286. Cf. U.S. CONST. art. I, § 9, cl. 8, § 10, cl. 1 (prohibiting, respectively, state and federal titles of nobility). The unamended Constitution denied few powers to both the state and federal government. I believe that only tariffs on interstate exports, bills of attainder, and ex post facto laws enjoyed the same dual prohibition.

287. Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 297-305 (1996).

288. *Compare Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417 (1984), *reh'g denied*, 465 U.S. 1112 (1985) (Betamax tape recorder facilitating unauthorized copying of television programs), *with A&M Records v. Napster*, 114 F. Supp. 2d 896 (N.D. Cal.) (granting plaintiff's preliminary injunction), *motion for stay of preliminary injunction granted by*, No. 00-16401, 2000 U.S. App. LEXIS 18688 (9th Cir. 2000) (Internet facilitating unauthorized copying of music).

289. Radin & Wagner, *supra* note 157, at 1303-06. These authors hint that the law of the domain name system is something more than trademark. Perhaps.

tive to distribute them rationally, as opposed to the land-rush aspects of domain-name registration. Similar, though perhaps more novel, is the emerging property law of hypertext links on the Web.²⁹⁰

There are two significant intellectual property issues we have yet to discuss. One of them—the business method patent—is not really a “law and technology” story, even though a number of Internet business methods have received very controversial patents.²⁹¹ Quite the contrary, the real question in business method patents is whether the patent system exists to reward technological innovation alone (“invention”), or social innovation in general. Does patent law really have anything to do with technology? Or to rephrase: is “technology” limited to natural and logical science? Is James Madison a greater inventor than Thomas Edison? Apart from noting that this is a very old issue in patent law,²⁹² I need not further discuss it.

2. *Digital Rights Management*

We finally discuss “digital rights management,” a phenomenon that goes by many names.²⁹³ As with the commodification of culture, this is a mixed story: technology and law intermediated by society. But here, the recent informatics technologies have played an instrumental role, closely coupled with legal issues.

This story begins with older informatics technologies: xerography, audio recording in the 1960s, and video recording in the 1970s. These new technologies permitted a far more rapid and inexpensive reproduction and dissemination of information than before. Because these new technologies were cheap and decentralized, anybody could make a copy, authorized or not. (In the language of Part III.A, the data structures became increasingly dissociated from their corresponding media, and the system boundaries

290. See Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609 (1998).

291. See, e.g., U.S. Patent No. 5,794,207 (issued Aug. 11, 1998) (Priceline.com's business method); U.S. Patent No. 5,960,411 (issued Sept. 28, 1999) (Amazon.com's One-Click business method).

292. Eighteenth-century English patent law tended to reward innovation in general, whereas U.S. patent law always concentrated on technological invention. E.B. INLOW, *THE PATENT GRANT* 1-43 (1950); *McClain v. Ortmyer*, 141 U.S. 419, 427-28 (1891). Seventeenth-century England took this to its logical conclusion. Any innovation was patentable, even if there were no novelty. See *Edgebury v. Stephens*, 2 Salk. 447 (1691) (“if the invention be new in England a patent may be granted, though the thing was practiced beyond sea before; . . . for the act intended to encourage new devices useful to the kingdom, and whether learned by travel or by study, it is the same thing.”). Related patent asperities are discussed *infra* note 309.

293. See Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management in Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 560 n.7 (1998).

were fuzzy.)²⁹⁴ Authorization was irrelevant (at least to consumers) because the copyright industry would not dare sue all consumers. The Supreme Court drove this point home in 1984, holding that copyright law did not bar the new technologies.²⁹⁵ Thanks to the technology of the 1960s and 1970s, copyright became less valuable than it otherwise would have been.

Two more recent technologies let copyright industries redress the changes wrought by the older technologies. First, new digital technologies created records that could be accessed repeatedly, but could not easily be copied. The first one was the unencrypted CD-ROM, which was far superior to the tapes onto which it could be copied. As tapes improved (and CD-ROMs or MP3s could be created at home), the CD-ROM lost its edge. However, new protective technologies, drawing on cryptanalytic techniques, have emerged. This newest set of technologies may, in effect, nullify the older copying technologies. These new technologies, however, are still nascent. Second, remote data networking allowed users to access information at a central repository (e.g., LEXIS-NEXIS). The enabling technology was probably the modem, but the Internet has proven a far more convenient means to the same end.

In other words, the new digital recording and encrypting technologies restrict copying of electronic records. Remote access facilitates metered access to electronic messages. A regime of controlled copying of records and metered access to messages does not need the aid of copyright infringement litigation. Mere denial of service is enough. The same is true with software that may be disabled by remote access.²⁹⁶

However, it is difficult to prevent all unauthorized copying of records, all unauthorized use of software, or all unauthorized conversion of messages to copy-able records. A technological fix is not enough to give copyright industries complete control of their information. Therefore, they seek to buttress the technological fix by legal means. License restrictions may control some users. Criminal or tort law may control mass-market abusers, completely unauthorized users, or those who abet these criminals or tort-

294. See *supra* text accompanying notes 83-87.

295. *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417 (1984), *reh'g denied*, 465 U.S. 1112 (1985).

296. See UNIF. COMPUTER INFO. TRANSACTIONS ACT §§ 815-16 (2000). I did not discuss the disabling remedy in my discussion of licensing, because it is clearly not novel. See, e.g., U.C.C. §§ 2A-525(3), 7-206(2), 7-210, 9-609(b)(2) (1999); *Flagg Bros. v. Brooks*, 436 U.S. 149 (1978). Despite the ancient provenance of this remedy, it was a very controversial one in the UCITA deliberations. E.g., Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1090 (1998).

feasors by providing them with technological aids.²⁹⁷ Of course, the law must authorize any technological fix (such as denial of service). This panoply of legal and technological controls is known as "digital rights management." Given the availability of criminal or tort remedies, this system is clearly one of property rights.

Perhaps none of the legal elements of digital rights management are new. As discussed above, some *ersatz* intellectual property rights have traditionally been created from whole cloth, with a contractual warp,²⁹⁸ sometimes with a weft of "self-help." Even those provisions of copyright law that seek to control technologies that disable digital rights management are reminiscent of the drug paraphernalia laws of the 1960s. But some of the combinations of elements may be novel.

In the old days, self-help consisted of anti-forgery technology (which protects authenticity), secrecy (which protects information), and certain specialized face-to-face methods of controlling copying (such as the old lawyer's trick: "you can't take notes").²⁹⁹ Modern self-help often resembles or calls on system rules: arguably, a transition from individual action to collective power. We are in the regulatory realm of "code,"³⁰⁰ which is a central component of digital rights management.

Second, digital rights management is far more precise than traditional intellectual property. A purchaser of a copyrighted book may read the book until it falls apart. A bookseller cannot meter use except by crude price-discrimination techniques: a cheap flimsy volume to appeal to the beach readers, and a leather-bound tome to appeal to devotees. Digital rights management could permit a separate fee to be charged for each reading or viewing. Because digital rights management has the potential to bar a secondary market, it facilitates price discrimination.

Finally, digital rights management, taken as a whole, threatens to displace large swathes of traditional copyright law, rather than merely supplement them. A copyright infringement action has many defenses, such as fair use³⁰¹ and first sale.³⁰² A breach of license contract action may have far fewer defenses, especially if a copyright was never part of the contract.

297. See 17 U.S.C. §§ 1201-05 (Supp. IV 1998) (control of those who develop technologies to circumvent digital rights management).

298. This issue had last been particularly significant in the early twentieth century. See *supra* notes 139-142 and accompanying text.

299. See Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEG. STUD. 393, 407 (1999).

300. See *supra* Part IV.A.2.

301. See 17 U.S.C. § 107 (1994).

302. See 17 U.S.C. § 109 (1994).

Put baldly, digital rights management may render traditional copyright law irrelevant. In this, digital rights management is novel, even if its legal components are not. The effect on copyright law can be enormous. Some observers welcome this trend; others deplore it.³⁰³

It is not my point to participate in this debate on the merits. This debate seems vigorous enough without any aid on my part. I only wish to put it in perspective. The conflict of viewpoints is real, but is neither new nor peculiar to “cyberlaw.” It is part of a larger and older struggle within intellectual property law: the struggle between a cultural-constitutive view of intellectual property, and a utilitarian view.³⁰⁴ Those who view intellectual property as utilitarian generally favor freedom of contract and self-help, for all the usual utilitarian reasons.³⁰⁵

It may be worth noting that intellectual property law strains the foundations of utilitarian analysis. Intellectual property law—especially copyright and trademark—creates commercial incentives to shape preferences. Most utilitarians become uncomfortable with such “endogenous” preferences that subvert the concept of utility. (Even a pious utilitarian may blanch at Huxley’s *Brave New World*.) On the other hand, the endogenous

303. “Welcoming” articles include Bell, *supra* note 293; Dam, *supra* note 299; Robert P. Merges, *The End of Friction: Property Rights and Contract in the “Newtonian” World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115 (1997); Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827 (1998). “Deploring” articles include Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of “Rights Management”*, 97 MICH. L. REV. 462 (1998); Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111 (1999); Jessica Litman, *The Tales that Article 2B Tells*, 13 BERKELEY TECH. L.J. 935 (1998); Report of the Committee on Copyright and Literary Property of the Association of the Bar of the City of New York: A Proposal of the National Conference of Commissioners of Uniform States Laws to Adopt a Proposed UCITA 17-21 (June 21, 1999).

304. Another author views the struggle differently: a war between “neoclassicists” (identical to my “utilitarians”) and “minimalists” (copyright haters). Netanel, *supra* note 287, at 286-88. He advocates a third view, very similar to my “cultural-constitutive” characterization. Professor Netanel is somewhat more sympathetic to copyright than many cultural-constitutive critics. However, I am interested more in motivation than position.

305. *E.g.*, Dam, *supra* note 299. Some restrictions on freedom of contracting in intellectual property can be justified in utilitarian terms. For example, alienable “moral rights” in copyright are arguably a form of consumer protection for “naïve” artists, who need to be explicitly told which sticks in the copyright bundle they are alienating. *Committee for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989); *cf.* U.C.C. § 2-316 (1999) (disclaimer of implied warranties must be conspicuous). A more sophisticated (and pervasive) utilitarian brief for restrictions may be found in Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121 (1999).

preferences problem looks less frightening when repackaged as “innovation.” After all, nobody wanted the zipper before it was invented. We will assume that the utilitarians can take care of their foundations, and look to their adversaries.

Utilitarianism is nearly irrelevant to many of those who view intellectual property as culturally or politically constitutive. Some authors try to reconcile the two positions, usually by asserting that properly understood utility just happens to be constitutive and cultural.³⁰⁶ But others argue that this circle cannot be squared.³⁰⁷ The cultural-constitutive view—which has dominated judicial rhetoric until recently³⁰⁸—is probably best known in copyright law, but has had a surprising impact on patent law, as well.³⁰⁹ Oddly enough, everybody favors pretending that trademark law has the drab utilitarian role of ensuring consistency of product, notwithstanding its central role in creating commercial culture.

The cultural-constitutive view has traditionally favored limited alienation of intellectual property rights,³¹⁰ and limited freedom of contract

306. *E.g.*, Cohen, *supra* note 303, at 544-559 (using microeconomic theory to attack digital rights management); Burk, *supra* note 305; Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

307. Netanel, *supra* note 287, at 325-336.

308. *See, e.g.*, George E. Marcus, *The Debate over Parody in Copyright Law: An Experiment in Cultural Critique*, 1 YALE J.L. & HUMAN. 295, 296 (1989) (“What are we to make of this gap between a rhetoric of copyright that embraces the majesty of the artistic creation and the obvious commercial contexts that have defined case law?”). However, it is no longer difficult to find a utilitarian copyright opinion. *See, e.g.*, Princeton Univ. Press v. Mich. Document Servs., Inc., 99 F.3d 1381 (6th Cir. 1996) (en banc), *cert. denied*, 520 U.S. 1156 (1997).

309. It is difficult to explain many traditional patent doctrines in utilitarian terms, such as the patent interference (unique to the United States), the inalienable right of the true inventor to have his or her name on the patent, or the low judicial deference traditionally granted the engineers at the Patent Office. (The recent case of *Dickinson v. Zurko*, 527 U.S. 150 (1999) at least put the technical expertise of engineers on a more equal footing with the social expertise of the lawyers or economists who inhabit other government agencies. This is an improvement, but normal people generally defer far more to engineers than lawyers or economists. Nobody crossing a bridge would think to ask to which political party its engineers belonged.) These odd patent doctrines can, however, be explained in terms of a non-instrumental goal of patent law: cultural valorization of invention, and more specifically, the inventor. *See* MARK TWAIN, A CONNECTICUT YANKEE IN KING ARTHUR’S COURT (1889); Joseph H. Sommer, *Nonobvious Doctrine: An Analysis of Patentability Law* (1994) (unpublished manuscript, on file with author). Many of these doctrines are disappearing, as patent law joins the utilitarian camp.

310. Moral rights, for example, are inalienable, at least on the Continent. 1 WILLIAM F. PATRY, COPYRIGHT 137 (1994); *see also* *Lear v. Adkins*, 395 U.S. 653 (1969) (holding patent licensee not estopped from disputing whether invention was patentable, allowing it

concerning intellectual property.³¹¹ The cultural-constitutive viewpoint has also favored a limited scope for intellectual property rights.³¹² Its adherents therefore look askance at attempts to create new intellectual property rights, especially if these rights are broad in scope. The utilitarians, in contrast, generally see no problem with new property rights in ideas and symbols, if the property rights are a necessary incentive to create or develop subsequently these ideas and symbols. I do not here wish to interject myself on either side of this debate, but merely wish to point out that there is nothing new here. Cyberspace is another battleground for an old war. However, the stakes may be higher, because all of copyright law may be at issue.

C. First Amendment

Much has been written about the Internet and the First Amendment. I have little to add, apart from my earlier comments on the public-private divide.³¹³ However, the First Amendment literature offers a lovely example of futurology.

A while ago, Liebling wrote “freedom of the press is guaranteed only to those who own one.”³¹⁴ The Internet might be lowering the cost of ownership, possibly in a socially significant way.³¹⁵ Perhaps the Internet will indeed ensure widespread dissemination and hearing of many viewpoints, unconstrained by the biases inherent in a press plutocracy. This raises at least three possibilities. One of these possibilities could be socially significant. Another could be doctrinally significant. Alas, the third possibility—which is the most drab—may also be the most likely.

to receive freedom from litigation inherent in license while suing). *Lear* is analyzed in Rochelle Dreyfus, *Dethroning Lear: Licensee Estoppel and the Incentive to Innovate*, 72 VA. L. REV. 677 (1986).

311. *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339 (1908).

312. For example, the courts have looked askance at state law efforts to expand traditional patent and copyright, holding that Federal patent and copyright laws preempt these efforts. *Bonito Boats v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989) (patent laws). Similarly, the Federal patent and copyright laws are constitutionally limited in scope. *See Feist Publ'ns, Inc. v. Rural Tel. Serv., Co.*, 499 U.S. 340 (1991) (copyright laws). It is perhaps worth noting that, since the New Deal jurisprudence of the 1930s, no other body of economic law (except commercial free speech) has been so heavily constitutionalized. *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974).

313. *See supra* Part IV.A.2.

314. A. J. LIEBLING, *THE PRESS* 32 (2d rev. ed. 1975).

315. This point was made at length by Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995). The *Harvard Law Review* coined the term “cyber-reach” to describe the power of an Internet user to “communicate and interact with a vast and rapidly expanding cyberspace audience.” *Developments, supra* note 152, at 1610.

The socially significant possibility, articulated by Volokh,³¹⁶ is that First Amendment reality will finally match First Amendment rhetoric: a vibrant marketplace of ideas, in which buyers and sellers can get together, unmediated by an oligopoly of intermediary press-lords. Perhaps the last time that buyers and sellers of ideas were unmediated by a few intermediary press lords was back in the eighteenth century: the glorious era of anonymous—and often ideologically significant—pamphleteering. This raises the second possibility, the doctrinally significant one. Perhaps if we return to an eighteenth-century marketplace of ideas, First Amendment reality and rhetoric may readjust to eighteenth-century standards. Remember that the Alien and Sedition Acts³¹⁷ regulated pamphleteering, and co-existed with the text of the First Amendment. Remember also the *Dennis* case, which survived a First Amendment challenge.³¹⁸ One could argue that we can indulge an expansive First Amendment rhetoric today only because the reality is so different: that wealthy (and hence the argument goes, responsible) press lords provide socially necessary censorship to the only communication media that matter. If the Internet breaks their oligopoly, one could argue that the governing law will change.

The third—and most likely—possibility can be explained with an established technology. Xerography, like the Internet, can reduce the cost of speech in a socially significant way. Many totalitarian societies keenly appreciated this threat, and closely regulated this subversive technology. However, xerography never seemed to make much difference to political speech in the United States. There may be a reason for this. The xerographic (or Internet) “press” may be cheap, but readers’ time remains expensive. In any reasonably free society, the supply of democratic discourse might far outstrip demand.³¹⁹ A vibrant marketplace of ideas is not worth much if all the vibrancy is on the supply side. It is worth remembering that today’s Internet users are far more willing to pay for pornography or real-time stock quotes than for Internet news and commentary—which does not bode well for the demand for unmediated political discourse.

Internet provocateur Matt Drudge has come and (mostly) gone, and the press lords remain. I’m betting on stasis. However, futurology is a dangerous business.

316. Volokh, *supra* note 315.

317. Ch. 54, 1 Stat. 566 (1798); ch. 58, 1 Stat. 570 (1798); ch. 66, 1 Stat. 577 (1798); ch. 74, 1 Stat. 596 (1798).

318. *Dennis v. United States*, 341 U.S. 494, 502 (1951) (holding that advocacy, unlike discussion, is not necessarily protected by the First Amendment).

319. Or technically, it might be far more elastic than demand.

VI. CONCLUSION

This Article has made one argument and told many stories. The argument is simple to summarize: neither “cyberlaw” nor the “law of the Internet” exists, neither *can* exist, and both concepts carry some dangers. Because technology and law are socially mediated, bodies of law do not respect technological boundaries, and technologies do not define law. Only if we consider the Internet to be a singular social phenomenon can we expect to see a “law of the Internet.” However, unless we limit our scope to Internet governance, the Internet is far too protean to support only a single set of social practices.³²⁰ Conversely, the Internet—as a mere technology—is far too narrow to dominate any interesting social practice that requires a governing body of law. The confusion of technology with social practice is a dangerous one, leading to parochialism, loss of history, and reductionism.

Let us forget about the “law of the Internet,” or “cyberlaw.” They cannot be useful, and may cause harm.

But what do we do with the stories? I have told many of them: many fields of law. Perhaps the individual discussions should speak for themselves. However, it cannot hurt to conclude with some tentative, modest generalizations.

First, novelty is rare. Consider digital rights management and electronic agents: the strongest candidates for novel law developed in this Article. Is digital rights management legally novel? Not really, say its proponents, not more so than freedom of contract in licensing. Are electronic agents legally novel? Perhaps no more so than the law of mistake or (for antiquarians) the Roman law of slavery.

However, novelty is a matter of perspective:³²¹

Knowledge after the event is always easy, and problems once solved present no difficulties, indeed, may be represented as never having had any, and expert witnesses may be brought forward to show that the new thing which seemed to have eluded the search of the world was always ready at hand and easy to be seen by a merely skillful attention.³²²

This quotation comes from a patent law case. Patent law is a law of significant (i.e., “nonobvious”) novelty, and some of its ideas might be useful here. Digital rights management may be a combination of familiar

320. See Wu, *supra* note 27.

321. See Hardy, *supra* note 154, at 996.

322. *Diamond Rubber Co. v. Consol. Rubber Tire Co.*, 220 U.S. 428, 435 (1911).

elements, but is novel enough to threaten the relevance of copyright. Even if electronic agency is “merely” the classic law of mistake, it is a truly surprising application of this old body of law to an unexpected context. I would grant a patent on both. But I might stop there. The law of domain names, for example, is not quite the law of trademark and unfair competition. But it is not all that different.

One should expect that legal novelty is the exception, rather than the rule. Bankers, for example have been working in cyberspace for a hundred and fifty years, since the telegraph. Unsurprisingly, by the 1930s, we had a workable law of electronic contracting. We somehow forgot this law of electronic contracting, or assumed that judges would not understand that the law of the telegraph was also the law of the Internet.³²³ In addition, by this time we also had workable choice-of-law rules for intangible rights created by electronic messages. The old choice-of-law rules were temporarily abandoned, although we have recently re-adopted them. We have long had complex governance structures of the networked information industry called banking, a governance structure that straddled the public-private divide. Although the cognate governance of the securities business has received some outside attention,³²⁴ only bankers are aware of these structures.

The same is true for jurisdictional issues. Again, nothing novel is presented by new technologies, albeit for different reasons. The driving force behind the law of personal jurisdiction has probably been the nationalization of our economy. To be sure, this has a technological basis (the railroad, the telephone, and the like), but the technologies themselves are once removed. As usual, society mediates law and technology. The law of international jurisdictional cooperation is another example. The driving force has been globalization, whose characteristic technologies are the jet plane and the telephone system. However, here at least, the Internet has had some effect, namely moving some traditionally wholesale problems to the retail market.

Second, precedent is quirky. Precedent is not the opposite of novelty. True, if something is not novel, it must surely have precedent. However, the converse is not always true. As discussed above, electronic agents with discretion seem novel. However, I have argued that the characteristic law

323. Certainly, some courts have made some stupid errors in the law of electronic commerce. See WRIGHT AND WINN, *supra* note 49, table 14.1 (compendium of cases, including judicial boners). But most courts got it right, as did most commentators. See 27 C.J. *Statute of Frauds*, *supra* note 103; 62 C.J. *Telegraphs and Telephones* *supra* note 151.

324. *E.g.*, Freeman, *supra* note 188, at 650-51.

of electronic agents is the well-established law of mistake. How could such an old law fit a fundamentally new legal problem? If you believe my argument, it fits this problem well. We have a puzzle here, which I cannot resolve.

Third, cyberspace is often not the Internet. Several of my stories are staples of the "cyberlaw" literature, yet had little to do with recent informatics technologies, and less to do with the Internet:

- 1) Enforcement and international cooperation is only secondarily an Internet story. Instead, it is primarily a story of globalization.
- 2) The structure of international banking law has not changed since the Russian Revolution. What had changed was legal thought. Legal realism erased the old choice-of-law rules and a more sophisticated legal reality restored them. It was only coincidence that the restoration occurred in the late 1980s and early 1990s.
- 3) The modern laws of records and messages have been around since the telegraph, and the Internet is merely bringing them to our attention.
- 4) As seen with sovereignty, the Internet has a way of bringing many old issues to our attention again. It does not thereby make them new issues.
- 5) Privacy is the law of the mainframe much more than of the Internet.
- 6) Digital rights management is only secondarily a law of the Internet. The primary relevant technologies appear to be xerography, the tape recorder, cryptanalysis, and the dialup modem. The Internet is only a better way of using the telephone dialup.

Fourth, new ideas can be sneaky. In 1908, the Supreme Court had to decide what a "copy" was. Player pianos were the technology *du jour*. They posed a novel legal problem. Sheet music was copyrightable. Player pianos did not read sheet music. Instead, they read special perforated paper scrolls. As the perforations passed by the playing head, an ingenious mechanism activated by the perforations struck the appropriate piano key. Was the perforated paper a copy of the sheet music? The majority said "no" while Justice Holmes said "yes."³²⁵ In response, Congress extended

325. *White-Smith Music Publ'g Co. v. Apollo Co.*, 209 U.S. 1, 18-20 (1908) (Holmes, J., concurring).

copyright protection to these paper scrolls the next year.³²⁶ The paper scrolls then became a copy of sheet music, even though they were only machine-readable.

What Congress and Justice Holmes did is noteworthy. They invented the concept of the medium-independent data structure, and held that it was the essence of copyright, regardless of whether the data structure was perceptible without special technological aid.³²⁷ In this, they disagreed with at least eight fine legal minds. It was a controversial issue then, but taken for granted today. At least, I think it is taken for granted. I took it for granted in my discussion of the law of records,³²⁸ and hope that the readers did, too.

The informatics revolution encourages examination of many legal practices. Most of these practices are sound, which may disappoint seekers of legal novelty. However, these practices will be stronger after examination. My analysis of the law of records and messages is to the point. This body of law is composed mostly of old doctrine, with some modest generalizations to fit a changed environment. It *could* have existed as a legal category in the old days. However, it was just too inconvenient and clumsy an idea in an era where one permanent medium—paper—was the norm. The camera and telegraph were idiosyncrasies that took to intuitive idiosyncratic rules. Evanescent media besides speech were almost irrelevant. The law of records and messages appears far more useful an idea today, when there are many competing media of which we must make comparative legal sense. Understanding our legal practices might not change a thing, because most of our practices are likely sound. Nevertheless, they will change the way we see these practices. Given that our legal practices are social constructs, this may be as much novelty as we will see.

I conclude with one final point. In many respects, cyberspace is no more unique than any other social practice or set of social practices. “Law and cyberspace” is similar to “law and [social practice of one’s choice.]” The discussion of sovereignty shows this point well. “Cyberspace and sovereignty” is not structurally dissimilar from “banking and sovereignty,” “globalization and sovereignty,” “shopping centers and sovereignty,” or the like. All draw on the same political theory and many of the same legal

326. See The Copyright Act of Mar. 4, 1909, ch. 320, 33 Stat. 1075.

327. Of course, sheet music is not necessarily perceptible without special technological aid. Eyeglasses are technologies, along with decent artificial lighting. This should suggest (at least to readers who did not object to the main text) that there is something special about technologies deemed universally accessible.

328. See *supra* text accompanying note 83.

sources. None have structural features that make them extraordinarily different from anything else.

But this does not mean that cyberspace and law is an unnatural combination, or is unworthy of study. Quite the contrary: cyberspace is a delightful new playground for old games. For example, we can learn much about the public-private divide from cyberspace, and our learning will illuminate far more than cyberspace.³²⁹ Or banking law, for that matter. But does this make cyberspace a special place? Recall William Blake's epitaph:³³⁰

To see a World in a Grain of Sand
And a Heaven in a Wild Flower,
Hold Infinity in the palm of your hand
And Eternity in an hour.

Cyberspace contains a tremendous wealth of legal learning, much of which is yet untapped. But so do many other things. Robert Ellickson on homeowners' associations may have just as much to teach about the public-private divide, although the lessons may be different.³³¹ Mark Lemley recently wrote a delightful and informative piece on the role and economics of norms in cyberspace, but was careful to credit cognate "role and economics of norms" work in many other fields.³³² Robert Cover's brilliant exploration of the tension between sovereigns and autonomous communities was guided by a tax exemption case.³³³

A sufficiently close and intelligent study of anything will illuminate everything else. This does not mean that everything is of equal significance. It just means that everything is connected. With enough attention and intellect, these connections can be teased out. The work is well worth doing. It is an antidote to both bigthink and overspecialization. It reminds us that beauty and insight may exist in unexpected places.

Yet a miniature is not a landscape, no matter how detailed. Some things remain bigger than others. We cannot infer that cyberspace is legally central simply because it so nicely illuminates some central legal

329. See Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

330. WILLIAM BLAKE, COMPLETE WRITINGS 431 (Geoffrey Keynes ed., 1972). These words are inscribed on Blake's tomb at St. Paul's chapel in Westminster Abbey.

331. Ellickson, *supra* note 175.

332. Lemley, *supra* note 171.

333. Cover, *supra* note 169. The case was *Bob Jones Univ. v. IRS*, 461 U.S. 574 (1983).

problems. All we can safely infer is that some very intelligent people like to think about the Internet.