Contracts in Cyberspace

by

David Friedman

School of Law and Department of Economics
Santa Clara University
ddfr@best.com
www.best.com/~ddfr/

May 4, 2000

Contracts in Cyberspace*

In modern societies contracts are enforced in two quite different ways: publicly, through the court system, and privately, largely through reputation. For a simple example of reputational enforcement, consider a department store that guarantees to refund your money if you are not satisfied. If, when you discover that the jacket you bought is the wrong size and your wife points out that purple is not really your color, the store refuses to give you a refund, you are very unlikely to sue them—the amount at stake is not enough to make it worth the time and trouble. Nonetheless, almost all stores in that situation will, at least in my experience, take the product back—because they want the reputation, with you and with other people you may discuss the incident with, of living up to their promises.

For a more elaborate example of reputational enforcement, consider the New York diamond industry as described in a classic article by Lisa Bernstein.[1] At one point, somewhat before the time she studied it, the industry had been mostly in the hands of orthodox Jews, forbidden by their religious beliefs from suing each other. They settled disputes instead by a system of trusted arbitrators and reputational sanctions. If one party to a dispute refused to accept the arbitrator's verdict, the information would be rapidly spread through the community, with the result that he would no longer be able to function in that industry. The system of reputational enforcement survived even after membership in the industry became more diverse, with organizations such as the New York Diamond Dealer's Club providing both trusted arbitration and information spreading.

The central thesis of this article is that, for contracts in cyberspace in the future, public enforcement will work less well and private enforcement better than for contracts in realspace at present. A secondary thesis is that while

---

* I would like to thank Bruce Benson for permitting me to read a manuscript of his which makes essentially the same argument as this article from a somewhat different perspective. I have felt free to avail myself of his references where they were relevant to my argument, and have included a number of relevant articles by Benson in the list of references at the end of this piece.

[1] Bernstein, Lisa, "Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry," 21 JOURNAL OF LEGAL STUDIES, 1992, pp.115-157.

the factors that make public enforcement less workable in cyberspace will not apply to contracts in realspace, the factors that make private enforcement more workable will. Hence we can expect some shift from public to private mechanisms for enforcing both realspace and cyberspace contracts, although the shift should be larger for the latter.

Problems with Public Enforcement in Cyberspace

Currently, commercial activity in cyberspace, mostly on the World Wide Web, is increasing rapidly. Such commerce poses two rather different problems for conventional mechanisms of public contract enforcement. One, which is likely to be important in the near future, is that cyberspace has no geographical boundaries. Purchasing goods or services from the other side of the world is as easy as purchasing them from your next door neighbor. Delivery of physical goods is more costly from the other side of the world—but a considerable part of cyberspace commerce is in information goods and services, and they can be delivered online just as they can be purchased online. It follows that an increasing fraction of commercial transactions, especially of transactions by private individuals, will be between parties in different countries.

Public enforcement of contracts between parties in different countries is more costly and uncertain than public enforcement within a single jurisdiction. Furthermore, in a world where geographical lines are invisible, parties to publicly enforced contracts will frequently not know what law those contracts are likely to fall under. Hence public enforcement, while still possible for future online contracts, will be less workable than for the realspace contracts of the past.

A second and perhaps more serious problem may arise in the future as a result of technological developments that already exist and are now going into common use. These technologies, of which the most fundamental is public key encryption, make possible an online world where many people do business anonymously, with reputations attached to their cyberspace, not their realspace, identities. [2]

[2] For a much more extensive discussion of these issues, see Friedman (1996).

There are a variety of reasons why people may in the future wish to avail themselves of such technologies. One is privacy; many people don't want others to know what they are reading, buying, or saying online.[3] A second is to evade taxes—it is hard for the government to collect taxes on activities it cannot see. A third is to evade regulations—whether commercial regulations in the U.S. or religious regulations in a country controlled by Muslim fundamentalists. Anonymity is likely to be particularly attractive to people living in parts of the world where property rights are insecure, making secrecy a valuable form of protection. If, for these or other reasons, a significant amount of commerce becomes anonymous, public enforcement of contracts will become increasingly irrelevant; it is hard to sue someone when you do not know who he is or what continent he lives on.

Private Enforcement of Contracts

What about the private alternative? At first glance, one might think that the same changes that made public enforcement of contracts more difficult in cyberspace would make private enforcement not only difficult but impossible. My local department store keeps its promises in part because if I am dissatisfied with their behavior, the people I talk to are likely to also be their customers; in a future without geography, where everyone is shopping everywhere, that is far less likely. And it is not obvious how you can injure someone's reputation without knowing his name.

Both of these problems are soluble; in each case, online commerce provides not merely substitutes for the reputational mechanisms with which we are already familiar but superior substitutes.

Consider first the problem of getting information from one customer to another. Considered as a mechanism for spreading information, local gossip is very much inferior to a well designed search engine. If, today, I am considering dealing with an online merchant and want to know whether other customers have had problems with him, I do not bother to ask either friends or the Better Business

[3] For a discussion both of the puzzle of why people favor more privacy, for others aw well as themselves, and of the relation between privacy and technology, see Friedman (2000).

Bureau. A one minute search with Deja News will tell me whether anyone on Usenet News has mentioned that firm any time in the past year, and show me what was said.

Online commerce is already institutionalizing such mechanisms. Consider eBay, a very successful online auction site. Their software permits anyone who has won an auction to post comments on the seller—whether the goods lived up to their description, were delivered promptly, or whatever else he wants to say. The comments are available, both in summary form and in text, to anyone bidding in an auction with that seller.

So far I have been considering informal reputational enforcement, the online equivalent of the reputational mechanism that keeps your local department store honest. What about formal enforcement, along the lines of the diamond industry? Here too, cyberspace has significant advantages over realspace.

To see why, it is worth thinking a little about how reputational enforcement works. The reason the department store, or the dishonest diamond merchant, is concerned about his reputation is not fear of being disliked but of losing business. The reason your friend will shop at another store if you tell him that this one refused to take your jacket back is not that he wishes to punish the store for cheating you but that he does not himself want to be cheated. Reputational enforcement works by spreading true information about bad behavior, information that makes it in the interest of some who receive it to modify their actions in a way which imposes costs on the person who has behaved badly.

How well that mechanism works depends on two things. One is the degree to which reputation matters; if I am a confidence man who plans to cheat you out of a million dollars and then retire, my future reputation is not very important. I don't care if anyone trusts me again. But most firms are in business for more than one transaction. Hence for most firms, a reputation for cheating their customers or other firms they do business with is a costly liability.

The other critical variable is the cost to third parties of obtaining reliable information about what happened. In most disputes, both parties claim that they are in the right and the other in the wrong. When I tell my friend how badly the

department store treated me he, hopefully, knows me well enough to decide whether or not to believe my story. But when I read a post on Usenet News criticizing a firm I do not have that sort of information about the author. I have to form my opinion based on internal evidence--does the poster sound reasonable--and consistency with other sources of information, such as other people posting in response.

For controversies with substantial amounts at stake, arbitration[4] provides a mechanism for lowering information costs to interested third parties. A New York diamond merchant does not have to know the details of a controversy—merely the verdict of the arbitrator as to who was at fault and whether or not the party at fault provided suitable compensation to the injured party. That system works because, even if the interested third party does not know the details of the controversy, he does know that the arbitrator is competent and honest. Computer technology provides an equivalent that requires considerably less information and functions at even lower cost.

Keys and Signatures: A Brief Digression

To explain how that equivalent works, I must first briefly sketch some relevant technology; readers already familiar with public key encryption and digital signatures may want to skip this section.

Public key encryption is a mathematical process for scrambling and unscrambling messages. It uses two keys, numbers containing information about a particular way of scrambling a message. The special feature of public key encryption is that if one of the two related numbers is used in the scrambling process, the other must be used in the unscrambling process. If I have one of the two keys I can encrypt my messages with that key, but someone who wishes to decrypt messages that have been encrypted with that key needs to use the other one. While a pair of such keys can be generated together, there is no easy way of calculating one of the two keys from the other.

---

[4] Some readers may associate arbitration primarily with institutions for settling disputes that are selected only after the dispute arises. In this article, my primary interest is in arbitrators chosen in advance--by parties when they sign a contract that might lead to future disputes.

To make use of public key encryption, one generates such a pair of keys. One, called your public key, you make available to anyone you might be corresponding with. The other, called your private key, you keep entirely secret.

Someone who wants to send you a message encrypts it using your public key; since only you have the matching private key, only you can decrypt it. Someone who wants to digitally sign a message encrypts it using his private key[5] and attaches unencrypted information identifying himself. The recipient obtains the sender's public key and uses it to decrypt the message. The fact that what he gets is a message and not gibberish demonstrates that it was encrypted with the matching private key; since only the sender possesses that particular private key, the digital signature authenticates the message.

Not only does a digital signature prove who sent the signed message, it also proves that the message has not been altered, and it proves both in a form that the sender cannot deny. If the sender tries to deny the message, the recipient can point out that he has a version of it encrypted with the sender's private key, something that only the sender could have produced.

Reputational Enforcement: Convincing Interested Third Parties

Imagine that you and I are signing a contract online, specifying our mutual rights and obligations for some substantial transaction. We include in the contract the name and public key of the arbitrator who we agree will settle disputes between us. We then both digitally sign the contract. Each of us gets a copy.

A dispute arises; I accuse you of violating the terms of the contract. We put the question to the arbitrator. He rules in my favor and instructs you to pay me $5000 in

[5] The process used for digital signatures in the real world is somewhat more elaborate than this, but the difference are not important for the purposes of this article. A digital signature is produced by using a hash function to generate a message digest—a string of numbers much shorter than the message it is derived from—and then encrypting the message digest with the sender's private key. The process is much faster than encrypting the entire message and almost as secure. It also means that it is possible to read the message without bothering to check the signature.

damages. You refuse. He writes up his account of what happened (he ruled in my favor and you refused to abide by his ruling), digitally signs it, and gives me a copy.

I now make up a package consisting of the original contract (digitally signed by both of us, and including the arbitrator's public key) and the arbitrator's account (digitally signed by him). I send the package to any third party who I think might want to know whether or not you are trustworthy—and post it on a web page with your name all over it, to be found by anyone searching for information about you. The third party (more precisely, his computer) checks the digital signatures on the contract and on the account, using the public key included in the contract to check that the account is by the arbitrator we agreed to. The third party now knows that you agreed to accept the ruling of that arbitrator and reneged on that agreement--and finding that out has taken him essentially no time at all.

Thus digital signatures provide a way of drastically reducing the cost to interested third parties of discovering whether someone is trustworthy,[6] and thus greatly increase the cost to individuals or firms engaged in repeat transactions of showing themselves to be untrustworthy by reneging on their contractual agreements.

Private enforcement of contracts along these lines solves the problems raised by the fact that cyberspace spans many geographical jurisdictions. The relevant law is defined not by the jurisdiction but by the private arbitrator chosen by the parties. Over time, we would expect one or more body of legal rules with regard to contract to develop, as common law historically did develop, with many different arbitrators or arbitration firms adopting the same or similar legal rules.[7] Contracting parties could then choose arbitrators on the basis of reputation.

---

[6] Strictly speaking, what the third party learns is that the accused either is not trustworthy or has agreed to use a dishonest or incompetent arbitrator. The latter alternative implies that while the accused may not be dishonest, save in the very limited sense of refusing to be bound by his own mistake, he is incompetent.

[7] As Bruce Benson has pointed out, this development is closely analogous to the development of the Lex Mercantoria in the early Middle Ages. That too was a system of private law enforced by reputational penalties, in an environment where state law was inadequate for contract enforcement, due in part to legal diversity across jurisdictions. See Benson (1998b,c)

For small scale transactions, you simply provide your browser with a list of acceptable arbitration firms; when you contract with another party, the software picks an arbitrator from the intersection of the two lists. If there exists no arbitrator acceptable to both parties, the software notifies both of you of the problem and you take it from there.

Private enforcement also solves the problem of enforcing contracts when at least one of the parties is, and wishes to remain, anonymous. Digital signatures make it possible to combine anonymity with reputation. A computer programmer living in Russia or Iraq and selling his services online has an online identity defined by his public key; any message signed by that public key is from him. That identity has a reputation, developed through past online transactions; the more times the programmer has demonstrated himself to be honest and competent, the more willing people who want programming done will be to employ him. The reputation is valuable, so the programmer has an incentive to maintain it–by keeping his contracts.[8]

Cheating in a Reputational System

There is at least one way in which the online world I have been describing makes contract enforcement harder than in the real world. In the real world, my identity is tied to a particular physical body, identifiable by face, finger prints, and the like. I do not have the option, after destroying my realspace reputation for honesty, of spinning off a new me, complete with new face, new fingerprints, and an unblemished reputation.

Online I do have that option. As long as other people are willing to deal with cyberspace personae not linked to realspace identities, I always have the option of rolling up a new public key/private key pair and going online with a new identity and a clean reputation.

[8] The first discussion of privacy through anonymity online of which I am aware of was in a work of fiction by a Computer Science Professor, Verner Vinge's novelette "True Names," included in *True Names and Other Dangers.* A good recent description of the combination of anonymity with online reputation occurs early in Marc Siegler's novel *Earthweb*.

The implication is not that reputational enforcement will not work but that it will only work for people who have reputations–sufficient reputational capital so that abandoning the current online persona and its reputation is costly enough to outweigh the gain from a single act of cheating. Hence someone who wants to deal anonymously in a trust intensive industry may have to start small, building up his reputation to the point where its value is sufficient to make it rational to trust him with larger transactions. Presumably the same thing happens in the diamond industry today.[9]

The problem of spinning off new identities is not limited to cyberspace. Real persons in realspace have fingerprints but legal persons may not. The realspace equivalent of rolling up a new pair of keys is filing a new set of incorporation papers. There is a well developed literature on the result, explaining marble facing for bank buildings and expensive advertising campaigns as ways of posting a reputational bond which makes it in a corporation's interest to remain in business, and hence gives others an incentive to trust it to act in a way that will preserve its reputation.[10] Cyberspace personae do not have the option of marble, at least if they want to remain anonymous, but they do have the option of investing either in a long series of transactions or advertising, in order to effectively bond future performance.

We are left with an obvious problem—how are entities not engaged in long term dealings to guarantee contractual performance in this world? The obvious solution is to piggyback on the reputation of another entity that is engaged in such dealings.

---

[9] *Earthweb* contains an entertaining illustration of this point. A central character has maintained two online personae, one for legal transactions, with a good reputation, and one for quasi-legal transactions, such as purchases of stolen property, with a deliberately shady reputation. At one point in the plot, his good persona is most of the way through a profitable honest transaction when it occurs to him that it would be even more profitable if, having collected payment for his work, he failed, at the last minute, to deliver. He rejects that option on the grounds that having a persona with a good reputation has just given him the opportunity for a profitable transaction, and if he destroys that reputation it will be quite a while before he is able to get other such opportunities.

[10] See, for example, Nelson (1974), Williamson (1983), Klein and Leffler (1981).

I am, again, an anonymous online persona forming a contract which may provide me an opportunity to benefit by defaulting on my contractual obligations. This time, however, I have no reputation, and no time in which to build one. Instead I offer to post a performance bond with the arbitrator—in anonymous digital currency,[11] assuming that I am seriously interested in protecting my own anonymity. The arbitrator is free to allocate all or part of the bond to the other party as damages for breach.[12]

This approach still depends on reputational enforcement, but this time the reputation belongs to the arbitrator. If he simply steals bonds posted with him, he is unlikely to stay in business very long. If I am worried about such possibilities, I can require the arbitrator to sign a contract specifying a second and independent arbitrator to deal with any conflicts between me and the first arbitrator. My signature to that agreement is worth very little, since it is backed by no reputation—but the signature of the first arbitrator to a contract binding him to accept the judgement of the second arbitrator is backed by the first arbitrator's reputation.

Conclusion

If the arguments I have offered are correct, we can expect to see a substantial shift in the direction of reliance on private enforcement via reputational mechanisms online, with an associated development of private law. To some degree, the same development can be expected in realspace as well. Digital signatures lower information costs to interested third parties whether the transactions being contracted over are occurring online or not. And the existence of a body of trusted online arbitrators will make contracting in advance for private arbitration more familiar and reliance on private arbitration easier for realspace transactions as well as for cyberpace transactions.

---

[11] For a discussion of how such currency would work, see Friedman and Macintosh (forthcoming).

[12] A real world version of this solution to the problem is the use of escrow agents by parties buying valuable goods on ebay.

Appendix: Some Simple Mathematics of Reputational Enforcement

I have claimed that an important determinant of how how well reputational enforcement works is how costly it is for interested third parties to determine whether or not a firm has cheated on past contracts. While this seems intuitively obvious, it is worth checking that intuition by formal analysis of at least a simple model.

Assume that there are many firms. Half of them are honest, half are amoral. An honest firm will never cheat by violating a contract; an amoral firm will cheat if and only if doing so increases its wealth--the present value of its profits from all transactions present and future.

Each time period, each firm gets an opportunity for a mutually profitable contract with another firm, chosen at random. If the firms agree to the contract and carry it out honestly, they each receive a profit π.

Each contract provides one of the two firms (which one chosen at random but known before the contract is signed) an opportunity to cheat--to violate the contract.[13] If it takes the opportunity, the cheating firm receives a profit π_C, the victim firm receives a profit π_V. I assume:

$\pi_C + \pi_V < 2\pi$ (cheating is inefficient)
$\pi_V < 0$ (a firm is better off not forming a contract if the other firm is going to cheat on it)
$\pi_C > \pi$ (a firm makes a larger profit by cheating than by not cheating)

Before forming a contract, a firm can pay a search cost $S>0$ to discover whether the other firm has ever cheated.

The game is played for ever.

Given these assumptions, how will firms behave? A firm that has an opportunity to make a contract where it is the one with a chance to cheat makes the contract without

[13] A firm that breaches a contract but pays damages according to the terms specified in the contract has not cheated in the sense in which I am using the terms. To cheat, it must both breach the contract and fail to pay any damages agreed on in advance or awarded by a pre-agreed upon arbitrator.

investigating the other firm, since whether that firm is honest does not affect the expected profit from the contract. A firm, honest or dishonest, that has an opportunity for a contract where it is the potential victim of cheating, will either:

1. Reject the opportunity
2. Accept it or
3. Spend S and then reject if the other firm has cheated, accept if it has not.

A dishonest firm with an opportunity to cheat must compare the gain from cheating-π_C -π-with the loss from a reduced opportunity to form contracts in the future, given that if it cheats once firms that investigate it will then decline the opportunity to contract with it.

What will the equilibrium of this system look like? One feature, given my assumptions, is that a firm either always cheats when it has the opportunity or never cheats. This follows from the assumption that what is discovered by investigating a firm is whether it has ever cheated. Given that assumption, once a firm has cheated it suffers no further reputational penalty from cheating again. So one feature of an equilibrium is $f_C \leq .5$, the fraction of firms that always cheat.

The second feature defining an equilibrium is the choice of strategies by firms that might be victims of cheating--what fraction of the firms (f_T) always trust the other firm, what fraction (f_D) always distrust, hence automatically reject any contract where they could be victims, and what fraction (f_I) investigate. Since those are the only possible strategies, we have:

$$f_T + f_D + f_I = 1$$

The condition for an equilibrium is that, for each of the two kinds of firms, each strategy that firm can choose yields the same expected return, with the exception of corner solutions--situations in which there is some strategy that that nobody is choosing that yields a lower return. The condition for a stable equilibrium is that if, starting with the equilibrium, a firm alters its strategy, the effect will be to make that strategy less profitable than some other strategy the firm might choose.

The relevant equations are:

Expected wealth of a firm = expected wealth from all cases where it is the potential victim plus expected wealth from all cases where it is the potential cheater.

Expected return from one case where it is the potential victim is

$\langle\pi\rangle_T=\pi \times (1- f_C) + \pi_V f_C$(Expected profit if it chooses to trust) (Eqn 1T)

$\langle\pi\rangle_D=0$ (If it chooses to distrust) (Eqn 1D)

$\langle\pi\rangle_S=\pi \times (1- f_C) -S$ (If it chooses to search) (Eqn 1S)

Expected return from one case where it is the potential cheater

$\langle\pi\rangle_N=\pi (1- f_D)$ (If it never cheats) (Eqn 2N)

$\langle\pi\rangle_C=\pi_C f_T$ (If it always cheats). (Eqn2C)

Suppose that $f_c=0$–nobody cheats. Since nobody is cheating, potential victims are always better off accepting contract opportunities without searching, so $f_T=1$. But that implies that cheating is always more profitable than not cheating, so $f_c=.5$. So there cannot be a corner solution at $f_c=0$.

What about the other corner solution for potential cheaters–$f_c=.5$? Solving for the behavior of potential victims, we have:

$\langle\pi\rangle_T=\pi \times (1- f_C) + \pi_V f_C= (\pi + \pi_V)(.5)$

$\langle\pi\rangle_D=0$

$\langle\pi\rangle_S=\pi \times (.5) -S$

So if $\pi+\pi_v>0$ (the profit from a successful contract is greater than the loss from being cheated) potential victims never distrust. Either:

$S>-\pi_v/2$,in which case potential victims always trust, or

$S<-\pi_v/2$,in which case potential victims always search, or

$S=-\pi_V/2$,in which case potential victims are indifferent between trusting and searching

But if potential victims always search, then cheating never pays, hence $f_C \neq .5$.

So the corner solution at $f_C=.5$ (everyone cheats who can) only exists if $S \geq -\pi_V/2$.

Next consider the interior solution: $.5>f_C>0$. Some potential cheaters cheat, some do not. Cheating would be unambiguously inferior to not cheating if no potential victims trusted, hence we must have $f_T>0$. Cheating would be unambiguously superior to not cheating if no potential victims searched, hence we must have $f_S>0$. So in order to have an interior solution, the value of f_C must be such that (from Equations 1T and 1S):

$$\langle\pi\rangle_T=\pi \times (1- f_C) + \pi_V f_C=\langle\pi\rangle_S=\pi \times (1- f_C) -S$$

Hence:

$$\pi_V f_C= -S$$

Put in words, the benefit of searching, the expected savings from not being a victim, must equal the cost. Hence:

$$f_C= -S/ \pi_V \qquad \text{(Eqn 3)}$$

If the parameters happen to be such that $\langle\pi\rangle_T = \langle\pi\rangle_S = \langle\pi\rangle_D=0$, which requires that

$$\pi= [S \pi_V]/ [S+ \pi_V] \equiv \pi^*$$

then an indeterminate number of potential victims will choose to distrust. But since it is only the relative proportions trusting and searching that determine the difference between the payoff from cheating and from not cheating, this does not affect the equilibrium value of f_C.

Combining Equations 2N, 2C, we have, for the interior solution:

$$\langle\pi\rangle_N=\pi (1- f_D) =\langle\pi\rangle_C=\pi_C f_T$$

$$\pi (1- f_D) = \pi_C f_T$$

So $f_T = \pi\ (1- f_D)/\pi_C$

Giving $f_T = \pi/\pi_C$ and $f_S = 1- \pi/\pi_C$ unless $\pi = \pi^*$.

We now have a solution:

$f_C^* = -S/\ \pi_V$, $f_T^* = \pi/\pi_C$, $f_S^* = 1- \pi/\pi_C$

Is it stable?

If f_c increases a little above f_c^*, the payoff to searching increases, the payoff to trusting decreases, so potential victims start to switch from trusting to searching. That lowers the payoff to cheating, pushing f_c back down. If f_T increases a little above f_T^* (and f_S decreases accordingly), the payoff to cheating increases, potential cheaters switch to cheating, that lowers the payoff to trusting, pushing f_T back down.

This is not a full formal analysis of the dynamics of the model–indeed it is hard to see in what sense one can talk rigorously of dynamics in my simple model, where once a firm has cheated its reputation is forever gone. But it looks as though the equilibrium is stable--or, if you prefer, would be stable in a slightly more complicated model in which firms occasionally vanish to be replaced by new firms, free to choose their reputation.

Equation 3 shows that the fraction of firms that cheat increases as search cost increases–indeed, is proportional to search cost in my simple model–until we reach $S=-\pi_v/2$, at which point we switch to the corner solution at $f_C=.5$, its maximum value.

So, at least in my simple model, my claim that lowering search costs makes reputational enforcement works better–fewer firms find it in their interest to cheat–is true.

References

Benson, B. L. (1998a). "Economic Freedom and the Evolution of Law." *Cato Journal*. 18, 209-232.

Benson, B. L. (1998b). "Evolution of Commercial Law." In P. Newman, (ed.). *The New Palgrave Dictionary of Economics and the Law*, London: Macmillan Press.

Benson, B. L. (1998c). "Law Merchant," In P. Newman, (ed.). *The New Palgrave Dictionary of Economics and the Law*, London: Macmillan Press.

Benson, B. L. (1998d). "How to SECEDE in Business Without Really Leaving: Evidence of the Substitution of Arbitration for Litigation." In D. Gordon. (ed.). *Secession, State, and Liberty*. New Brunswick, NJ: Transaction.

Benson, B. L. (1999). "To Arbitrate or to Litigate: That is the Question," *European Journal of Law and Economics.* 8, 91-151.

Benson, B. L. (2000). "Arbitration." In B. Bouckaert and G. De Geest. (eds.). *The Encyclopedia of Law & Economics*. London: Edward Elgar.

Bernstein, Lisa, "Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry," 21 *Journal of Legal Studies*, 1992, pp.115-157.

Choi, Stephen J., "Gatekeepers and the Internet: Rethinking the Regulation of Small Business Capital Formation," *The Journal of Small and Emerging Business Law*, Volume 2 (Summer 1998) Number 1 [http://www.lclark.edu/~lawac/LC/jsebl/summer98.htm]

Friedman, David, A World of Strong Privacy: Promises and Perils of Encryption," Social Philosophy and Policy (1996), pp. 212-228. [http://www.best.com/~ddfr/Academic/Strong_Privacy/Strong_Privacy.html]

Friedman, David, "Privacy and Technology", *Social Philosophy and Policy.* 17:2 (Summer 2000)

Friedman, David and Macintosh, Kerry, "Technology And The Case For Free Banking ," to be included in a forthcoming book edited by Dan Klein and Fred Foldvary.

Klein, B. and Leffler, K. (1981). "The Role of Market Forces in Assuring Contractual performance," *Journal of Political Economy*. 89, 615-641.

Nelson, P. (1974) "Advertising as Information," *Journal of Political Economy* 76, 729-754.

Siegler, Marc, *Earthweb*, (Baen Books: 1999).

Vinge, Verner, "True Names," included in *True Names and Other Dangers.*

Williamson, O. E. (1983) "Credible Commitments: Using Hostages to Support Exchange," *American Economic Review*. 83, 519-540.