1-1-2005

From Imperial China to Cyberspace: Contracting Without The State

David D. Friedman
Santa Clara University School of Law, ddfrr@daviddfriedman.com

Follow this and additional works at: http://digitalcommons.law.scu.edu/facpubs
Part of the Contracts Commons

Automated Citation
David D. Friedman, From Imperial China to Cyberspace: Contracting Without The State, 1 J.L. Econ. & Pol'y 349 (2005), Available at: http://digitalcommons.law.scu.edu/facpubs/6
FROM IMPERIAL CHINA TO CYBERSPACE: CONTRACTING WITHOUT THE STATE

David D. Friedman, Ph.D.*

I. THE PAST AS PROLOGUE

In 1895, as part of the treaty of Shimonoseki, China ceded the island of Taiwan to Japan. The Japanese government wished to maintain the existing legal system; in order to do so it had to discover what that legal system was. A scholarly commission was established, and its report provides us with a detailed picture of the legal system of at least one province of Imperial China at the end of its last dynasty (Brockman 1980, p. 130).1

One feature of that legal system was the combination of elaborate contractural practice with an almost total absence of contract law. Imperial China had no equivalent of our civil lawsuits. A merchant who had sold goods on credit and not been paid could, if he wished, report his debtor to the district magistrate for the crime of swindling him—but once he had done so, the case was out of the merchant’s hands. The magistrate, if convinced of the justice of the claim, might compel repayment—usually only partial repayment. He might do nothing. He might even conclude that the merchant was the one at fault and sentence him to a beating. The legal system enforced by the magistrate focused almost entirely on criminal acts and criminal punishment, with only a handful of provisions dealing with matters of contract (Brockman 1980, p. 85),2 and some, such as the statute specifying a maximum interest rate, appear to have been ignored in practice.

* Professor of Law, Santa Clara University. I would like to thank Bruce Benson for permitting me to read a manuscript of his which makes some of 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. An earlier version of part of this chapter was published in the Journal of Internet Law (Friedman 2002).

1 “The major publication in the area of customary law was Taiwan Shiho [the Private Law of Taiwan] (1910), a six-volume work which reprinted and analyzed documents pertaining to land law, family law, personal property and commercial law... with seven volumes of reference materials...”

2 “Of the 346 statutes in the Code, only eight dealt at all with what is usually called commercial law.”
The Chinese empire relied heavily on non-state hierarchical structures to maintain order and settle disputes, most notably the extended family, and it supported them in doing so (Bodde and Morris 1967). That provided a possible mechanism for settling contract disputes within family, clan or guild. But merchants in Taiwan engaged in extensive large scale dealings that cut across all such categories, buying bulk agricultural products to ship across the straits to be sold in the mainland, importing mainland products to Taiwan, and much else.

The problem of settling commercial disputes without state courts was dealt with in medieval Europe, in part, by the development of private courts at the major trade fairs, run by merchants and relying heavily on reputational enforcement (Benson 1998c). No equivalent seems to have developed in China, perhaps due to Imperial hostility to any rival authority.

Nonetheless, Chinese merchants developed an elaborate set of contractual forms, including a variety of form contracts, supporting an extensive and sophisticated network of commercial relations. Part of the explanation of how they did so was presumably the existence of reputational enforcement, part the availability of state courts for dealing, when all else failed, with parties engaged in deliberate and obvious violations. But much of the explanation lies in the details of the private contract law that developed within that framework—a system of rules designed to minimize the reliance on courts and external enforcement.

One example is the rule that we call caveat emptor. Under any circumstances short of clear and deliberate fraud—gold bars that turned out to be gold plated lead, for example—a merchant who had accepted delivery of goods had no recourse if they turned out to be defective. Another is the linkage between possession, ownership, and responsibility; goods in my warehouse were mine, whether or not they were about to become yours, and I bore the risk of any damage that occurred to them.3 The rules appear to have been designed, wherever practical, to let a loss lie where it fell, thus eliminating the need for legal action to shift it.

Problems arise in situations where canceling a contract and leaving everything in the possession of whoever, at the moment, has it will advantage one party, a situation that encourages opportunistic breach. One solution is to redesign the contract so that the two parties' performance is more nearly synchronized, reducing the incentive of either to breach. An alternative is to rely on reputational enforcement, structuring the contract so that the incentive to breach, if it occurs, is likely to be on the party who will suffer reputational penalties from breaching.

An example in the Chinese case is provided by contracts for future purchase of commodities at a pre-arranged price. Such contracts were not considered binding until there had been at least partial performance by one

3 There were a few exceptions—most notably for a dye shop that would have cloth in it to be dyed.
party. Typically, that consisted of a deposit paid in advance by the purchaser. By adjusting the size of the deposit, the parties could take account of both how large the incentive of the seller to breach might become—depending on the range of likely price changes between contract formation and delivery—and how much each party was constrained to keep to the deal by reputation.

A buyer who breached forfeited his deposit—a result that required no judicial intervention, since the deposit was in the possession of the seller. That left an obvious problem—a seller who breached but kept the deposit. Presumably that was prevented by some combination of reputation and the threat that such an obviously criminal act would provide the buyer sufficient grounds for going to court.

Important elements in making the system work were the existence of a system of written forms using standard boilerplate terminology understood by the parties and others in the trade, and the use of seals—“ chops” —to provide clear evidence of assent to a contract. So long as issues of fact were simple—whether a shipment of grain had been delivered and accepted, but not the precise quality or quantity—it was possible for third parties to determine, at a low cost, which party to a contract had violated its terms. Here the third party might be either another merchant interested in knowing who could be trusted or, in extreme cases, a district magistrate interested in who had committed a criminal offense and should be punished accordingly.

Whatever the mechanisms responsible—interested readers can find a more detailed account in Brockman’s chapter—Chinese merchants a century ago succeeded in maintaining a sophisticated system of contracts with very nearly no use of state enforcement. It is the thesis of this paper that the past of China is our future—that parties to online transactions will, over the next few decades, face essentially the same problem and find, mutatis mutandis, similar solutions.

Both the Chinese past and the cyberspace future are special cases of a more general problem—contract enforcement in the absence of state enforced contract law. That problem appears in a variety of other contexts, including criminal markets and political markets. Perhaps less obviously, it appears in markets where court enforcement, although legally possible, is impractical because performance is difficult or impossible to monitor. The marriage market is an important example. For instance . . .

Al-Tannuhki, a 10th century judge, tells the story of a vizier who gave a large sum in alms, 200 dinar, to a poor woman. Three days later he received a petition from the woman’s husband, reporting that she had decided she was now too rich to be married to a poor man like him and was threatening to force him to divorce her. The husband asked the vizier to appoint some man in authority to prevent his wife from doing so. The vizier considered the problem briefly, took out paper and pen, and wrote “pay this man 200 dinar” (Margoliouth 1922).
It is possible for state courts to enforce rules permitting or restricting divorce. It is a great deal harder for them to enforce the other terms, explicit or implicit, of the marriage contract—to sanction someone for not doing a good job of being a wife or husband, even if the failure is deliberate. Given that difficulty, legal rules designed to punish one party for explicitly breaching the contract by getting a divorce may merely give that party an incentive to breach the less observable terms of the contract in order to make it in the other party's interest to agree to terminate it. That problem appears to have existed even in a medieval society whose marriage law was, on the face of it, heavily biased in favor of the husband.

Part II of the paper presents a general approach to private contract enforcement, some features of which are illustrated in the Chinese example. Part III sketches out the reasons why I expect that, for transactions in cyberspace, state enforcement of contracts will work worse and reputational enforcement better than in realspace today, including the technologies that provide an online equivalent of the seals used by Chinese merchants to establish the identity of a signatory party at a distance, in time or space. I go on to discuss how, in that environment, parties might structure their dealings, as well as the difficulties they will face due to the special nature of the cyberspace environment.

II. ENFORCING CONTRACTS WITHOUT THE STATE

Two parties wish to form a contract in a context where enforcement through a state court system is not a practical option. One simple way of doing so is the silent auction, for which we have descriptions going back to the sixth century B.C.\(^4\) One party piles up the goods he wishes to sell, the other makes a matching pile of what he offers in exchange. If the offer is acceptable, the first party takes the second pile and leaves the first, and if not, the first party adjusts his offer. The process continues until one party accepts the other's most recent offer.

No common language is required for this simplest form of auction, but the parties still need some way of enforcing their property rights, of preventing one of them from taking both piles and departing. That might be either the threat of violence or the discipline of repeated dealings—the expectation that if one party acted that way this year, the other would not show up next year.

Difficulties arise when what the parties are contracting for is performance, by one or both, spread out over a period of time. Lloyd Cohen has discussed that problem in the context of modern marriage law, where the combination of a shift to no fault divorce and a pattern of traditional marriage within which the wife's performance of her part of the joint duties

\(^4\) By Cosmas Indicopleustes and in the fifth century B.C. by Herodotus.
was concentrated in the early years of the marriage, the husband’s more heavily weighted towards the later years, provided an incentive for opportunistic breach by the husband (Cohen 1987).

A partial solution in that case was for the wife to postpone childbearing and shift part of the cost of child rearing from household to market, thus aligning her performance more closely with the husband’s. In a less intimate context, contractors building a house expect to receive payments spaced out over the time of construction and at least roughly corresponding to the spacing of costs, reducing the incentive of a contractor paid in advance to skip out with the money or a home owner promising to pay on completion to renege.

This kind of solution works reasonably well as long as the joint gains from final completion of the contract are substantial relative to the costs. Consider, however, the limiting case in the other direction—a situation where the gain to one party from breach is just equal to the loss to the other.

In such a situation, any departure from perfectly synchronized performance gives one party or the other an incentive to breach. If I have paid the contractor a little more than he has spent so far, he has an incentive to breach; if I have paid him a little less, I do. A more realistic example, and one which seems to have been a serious issue in the Chinese case, is a contract for future delivery at a pre-agreed price. If the transaction cost of arranging a replacement supplier is low, any significant drop in price provides an incentive for the buyer to breach; if the costs of finding a replacement buyer is low, any significant increase provides an incentive for the seller to breach. The parties can guard against breach by the buyer by having him pay a deposit in advance, but that increases the incentive for breach by the seller.

One solution is to create an artificial gain from completion—a cost to breach—by making it possible for the victim of breach to unilaterally impose a large cost on the other but not a correspondingly large benefit on himself. The deposit is replaced by a hostage. The threat of destroying the hostage reduces the gain to breach by the party who has given the hostage without creating a proportional increase in the gain to breach by the party holding the hostage. The logic of the situation is illustrated by Figures 1a-1c.

Figure 1a shows the situation with neither deposit nor hostage. The horizontal axis is time, starting just after the contract is negotiated. The vertical axis shows, for each party, its gain to breach—how much better off it will be if it breaches at that time than if the contract is completed. At time zero, the parties have negotiated the contract but no performance has occurred and no deposit has been made. Assuming that there was some cost to negotiation, which the parties expected to at least recover on completion of the contract, both parties should be worse off breaching at that point than carrying the contract to completion.
Over time, each party bears costs of performance which it expects to recover on completion, pushing the gain from breach further down, as shown between $t=0$ and $t=10$. At some point, possibly before completion, each party starts to get benefits from the partial performance that has occurred, increasing the gain (i.e. reducing the loss) from breach. In the figure, Party 1 is continuing to bear costs of performance from $t=10$ to $t=20$. Party 2 is no longer bearing costs of performance but is receiving benefits. So the gain to breach is falling for Party 1 but rising for Party 2.

If the contract is badly designed, at some point Party 1’s benefit to breach rises above zero. In a world with no enforcement of contracts, legal or reputational, Party 1 breaches—perhaps immediately, perhaps with a delay to let the gain rise even higher. In the Figure, that happens at $t=20$. Party 1’s gain is smaller than Party 2’s loss, so the breach is inefficient.

The parties can try to avoid such an outcome in the initial agreement by having Party 1 make payments to Party 2 between $t=10$ and $t=20$, shifting some of the gain from breach and keeping both parties’ gain from breach negative. But in an uncertain and imperfectly observable world, this may not always work, since the parties do not know with certainty what the pattern of either performance costs or benefits will be.

Figure 1b shows the same contract, with one change—at $t=0$, Party 1 pays a deposit $d$ to Party 2. That shifts Party 1’s gain from breach down, since if the contract does not go to completion the deposit will remain with Party 2; it is now no longer in Party 1’s interest to breach the contract. Unfortunately, it also shifts Party 2’s gain from breach up, since Party 2 can breach and keep the deposit. The result is that it is now in the interest of Party 2 to breach the contract—in this example, immediately after signing it and receiving the deposit.⁵

Figure 1c shows the same contract again, this time with Party 1 giving Party 2 a hostage rather than a deposit. The result is to shift Party 1’s gain from breach down without shifting Party 2’s gain from breach up, so neither party has an incentive to breach the contract.

---

⁵ The situation without the deposit or hostage is shown by the grey lines on figures 1b and 1c.
One example of this approach is the literal hostage, offered by one party in a conflict as a guarantee that he will abide by terms agreed to. For a less obvious equivalent, consider the role of the state court system in Taiwan. If a merchant failed to either deliver the goods contracted for or return the buyer's deposit, the buyer could report him to the district magistrate as a swindler. The resulting legal case might or might not provide any benefit to the buyer but was likely to impose large costs on the seller. From the standpoint of the strategic situation of the two parties, the threat to make use of the court served the same function as the threat to execute a hostage.

A similar situation arises in a world without courts, but in which parties are concerned about their reputation. When you cheat me, I gain very little by making the fact public. But, assuming my report is credible, you lose a great deal. That fact, combined with a credible commitment on my part to report breach, increases the net cost of breach and so reduces the risk
that breaching will be in the interest of one of the parties. Both this case and the previous have an additional attractive feature: the existence of the hostage depends at least in part on the existence of breach, since the accusation of breach, whether to the court or to the general public, is more damaging if true.

For a final example, consider the enforcement of contractual agreements in modern criminal markets. Antonio pays Ricco $100,000 for a large container of what turns out to be talcum powder. Antonio pays a hit man an additional $10,000 to kill Ricco—after first prudently convincing the local capo of the justice of his case in order not to get a reputation as a dangerous man to do business with but only a dangerous man to cheat. Here Ricco is, in effect, hostage for his performance—and Antonio for his.

It may occur to readers familiar with Coase that there is a problem with the use of hostages as a solution to the problem of opportunistic breach. The son I give as a hostage may be of no value to you, but he is of considerable value to me. If you decide to breach our agreement, you also inform me that you will kill him unless I buy him back from you for a suitable price. Similarly, if we are merchants in Taiwan, you breach the contract and then offer to buy my silence. You thus convert the hostage back into a deposit, eliminating the wedge between the terms on which it pays me to breach and the terms on which it pays you to.

Nonetheless we observe the use of hostages in contexts where a deposit would be of little use. One explanation is that parties who wish to give hostages are able to commit themselves not to accept such offers. Another is that the situation sets up a bilateral monopoly bargain with a large bargaining range and such bargains are likely to generate substantial transaction costs. That said, the issue deserves further thought.

The discussion of hostages brings us to the last and, for this purposes of this paper, most interesting mechanism for enforcing contracts without the state—reputation.

Reputational Enforcement

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

---

6 This point was suggested to me by R.C. Friedman.
7 This problem parallels a similar issue in the use of inefficient punishments, such as imprisonment, in criminal law as a way of reducing the risk of setting off a rent seeking struggle as some people attempt to use control of the criminal law to expropriate others. Thus we sometimes observe an inefficient punishment converted into a less inefficient punishment when police or prosecutors let one criminal off in exchange for testimony (true or false) that will allow them to convict another (Friedman 1999).
wife points out that purple is not really your color, the store refuses to give you a refund, you are 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, consider the New York diamond industry, as described in a classic article by Lisa Bernstein (Bernstein 1992). 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 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 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 those 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, a very large collection of online conversations, 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.

If I claim that you cheated me, and you claim that I cheated you, a third party who cannot easily find out which of us is telling the truth is
likely to attribute some probability to both stories—and avoid doing business with either of us in the future. It follows that if you have cheated me, but I cannot easily demonstrate the fact to an interested third party, I may be better off saying nothing, since complaining will lower my reputation as well as yours. This raises a serious problem of incentive compatibility for a system which depends on action taken, not by government employees hired to enforce the law, but by private individuals acting in their own self-interest.  

One way of lowering information costs to third parties is to have a legal system where the obligations of the parties depend on easily observed facts—loosely speaking, a system of bright line rules rather than standards. That appears to describe some features of the Chinese system already discussed.

For controversies with substantial amounts at stake, arbitration\(^8\) provides a second 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. As we will see, computer technology provides an equivalent that requires considerably less information and functions at even lower cost.

**Cheating on the Reputational Bond**

There is another problem, however, which is likely to be more serious for online commerce than for the traditional realspace version. My current reputation functions as a bond to guarantee performance—if I cheat on a contract, I lose (or reduce) the reputation, which is costly. It follows that I will not cheat unless the gain from doing so is more than the value of the forfeited bond. If my reputation is worth a million dollars to me, you should be safe in trusting me up to that sum—in, for example, lending me $600,000.

I borrow $600,000 from you. I also borrow $400,000 from another lender and $500,000 each from two more. I then default on all the loans, forfeiting my million dollar reputation—in exchange for $2,000,000.

---

\(^8\) Friedman (2002), on which this article is in part based, includes a simple model of reputational enforcement showing the link between cost to third parties and the amount of cheating.

\(^9\) 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.
In order for reputational enforcement to work, the party who relies on it must have some way of knowing not only what opportunities the other party has to cheat him but what opportunities he has to simultaneously cheat other people. That may not be too much of a problem in the sort of ordinary market where most of the players know each other—before agreeing to lend me $600,000 you first discuss the situation with other potential lenders. But it could be a very serious problem for anonymous dealings online in a worldwide marketplace. In order for reputational enforcement to work in that setting, we need either an environment where the sort of opportunities made possible by my particular reputation are scarce enough so that I am unlikely to have a chance to take many at once, or procedures sufficiently transparent so that someone who relies on my reputation can know how many other people are currently doing so—how far I am stretching my reputational bond.

Whose Reputation?

A contract involves at least two parties, but they do not both have to have reputations. One is normally enough, since the parties can usually structure the contract to put the risk of breach on whichever can best bear it. If you are performing a service for me and I trust you but you do not trust me, because you are a repeat player with a reputation and I am not, I pay in advance. Reverse the situation and I pay on completion. In ordinary commerce, individual purchasers pay for goods when they get them, in the expectation that if the computer in the box turns out to have no innards, the store will take it back. The seller, in almost any field, is a repeat player with a reputation—the buyer often is not.

What about the situation where neither player has a reputation? In that case, they can solve the problem by bringing in a third party who does. An escrow agency provides a familiar example. I agree to pay you $50,000 for a sixteenth century painting by a known artist which you are offering on eBay. You deliver the painting to an escrow agency. I inspect it. If it fits the description I send you the money and claim the painting, if it does not the agency sends it back to you. Neither of us has to trust each other—only the agency. The mechanism does not depend on the existence of state courts to enforce the agreement, only on a third party with an adequate reputation.

III. PROBLEMS WITH PUBLIC ENFORCEMENT IN CYBERSPACE

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, already important, 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 some 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, largely based on public key encryption, make possible an online world where many people do business anonymously, with reputations attached to their cyberspace, not their realspace, identities (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 do not want others to know what they are reading, buying, or saying online. A second is to evade taxes; it is hard for a 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 (Friedman 2004). 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

---

10 For a discussion both of the puzzle of why people favor more privacy, for others as well as themselves, and of the relation between privacy and technology, see Friedman (2000).
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 Bureau. A one minute search with Google 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. 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, as described by Bernstein (Bernstein 1992)? Here too, cyberspace has significant advantages over realspace.

**Keys and Signatures: A Brief Digression**

To explain how the cyberspace equivalents of arbitration by the Diamond Dealer Club of New York and verification by the use of seals in 19th century China work, 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 the pair of keys is generated together, there is no easy way of calculating one of the two keys from the other.

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 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. Thus the digital signature in cyberspace serves the same function as the physical seal used to authenticate contracts in China a century ago—to prove authorship and responsibility at a distance in space or time.

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.

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 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

---

11 The process used for digital signatures in the real world is somewhat more elaborate than this, but the differences 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.
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.

Digital signatures provide a way of drastically reducing the cost to interested third parties of discovering whether someone is trustworthy.\(^{12}\) By doing so, they increase the cost to individuals or firms engaged in repeat transactions of 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 bodies of legal rules with regard to contract to develop, with many different arbitrators or arbitration firms adopting the same or similar legal rules.\(^{13}\) Contracting parties could then choose arbitrators on the basis of reputation.

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.\(^{14}\)

\(^{12}\) 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.

\(^{13}\) 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 (Benson 1998b,c).

\(^{14}\) 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, Vernor Vinge’s novelette “True Names.” A good recent description of the combination of anonymity with online reputation occurs early in Marc Siegler’s novel Earthweb.
Cheating in a Reputational System

There are, unfortunately, ways in which the online world I have been.
describing makes contract enforcement harder than in the real world. One
is that, 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 reputa-
tion.

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.

The implication is not that reputational enforcement will not work but
that it will only work for people who have reputations—sufficient reputa-
tional capital so that abandoning the current online persona and its reputa-
tion is costly enough to outweigh the gain from a single act of cheating.
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. Pres-
umably the same thing happens in the diamond industry today.

The problem of spinning off new identities is not limited to cyber-
space. 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 advertis-
ing campaigns as ways of posting a reputational bond that makes it in a
corporation’s interest to remain in business and hence gives others a reason
to trust it to act in a way that will preserve its reputation (Nelson 1974; Wil-
liamson 1983; Klein and Leffler 1981). 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 in a long series of transactions, or advertising,

---

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

16 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 transac-
tions, 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; if he destroys that reputation it will be
quite a while before he is able to get other such opportunities.
or some other publicly visible expenditure, in order to bond future perfor-
performance.

What if only one of the parties to an online contract is a repeat dealer
with a reputation? The solution, as in realspace, is to structure the contract
so that it is not in the other party's interest to breach it. The simplest exam-
ple is the purchase of goods or services. The party who does not have a
reputation performs first—pays in advance if he is the buyer, delivers in
advance of payment if he is the seller.

We are left with an obvious problem—how can a pair of entities nei-
ther of which is engaged in long term dealings guarantee contractual per-
formance in this world? One solution has already been mentioned—
piggyback on the reputation of another entity that is engaged in such deal-
ings.

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 arbitra-
tor—in anonymous digital currency, assuming that I am seriously inter-
ested 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.

This approach still depends on reputational enforcement, but this time
the reputation belongs to the arbitrator. If he steals bonds posted with him,
he is unlikely to stay in business very long. If I am worried about such pos-
sibilities, 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 con-
tract binding him to accept the judgment of the second arbitrator is backed
by the first arbitrator's reputation. For a less extreme example of the same
approach, consider the current use of escrow agencies for transactions on
eBay.

As that final example suggests, it is possible to combine realspace and
cyberspace institutions, state and private enforcement mechanisms. If court
enforcement in realspace turns out to provide a more reliable mechanism
than reputational enforcement online, anonymous online parties can use
identifiable real space third parties as escrow agencies, arbitrators, and in
other contexts in which a trusted third party eliminates the need for trust
between the other parties to a transaction. If, on the other hand, courts
prove less reliable, realspace parties can make use of online reputational
mechanisms instead—as they now do.

As long as parties are identifiable in realspace, the state has the option
of imposing its own terms on them—an option some parties may wish to

---

17 For a discussion of how such currency would work, see Friedman and Macintosh (2001, 2003).
avoid. But anonymous parties in cyberspace who wish to make use of a trusted third party in realspace can choose which third party, and hence which state, they wish to deal with. States will thus be constrained by competition in their dealing with online personae, just as U.S. states are currently constrained in dealing with corporations.

One way of succeeding in that competition is to make it possible for online parties to take advantage of realspace enforcement without revealing their realspace identities. A possible approach would be for a state to recognize transfers of claims from cyberspace to realspace persons, validated by the former’s digital signature. So if anonymous X has a valid claim against realspace Y, X sells the claim to realspace Z who prosecutes it—without either Z or the court having to know X’s realspace identity.

One problem with reputational enforcement online is that a party can roll up additional identities. A second problem is that a party can conduct multiple transactions, each invisible to those party to the others. As discussed earlier, that means that a party with a million dollar reputation might put together a collection of transactions, each of which was not worth cheating on (and forfeiting the reputation) but which together were.

One solution is to have a million dollar reputation and engage in thousand dollar transactions in a context where one is unlikely to be able to run as many as a thousand of them at once. In realspace that is often practical. It may work less well in cyberspace, where the identity of the party behind a reputation, including how many actual persons that party consists of, may be unknown.

An alternative is for a party to deliberately create transparency in order that everyone who contracts with him will be aware of the existence (but not necessarily the identity) of everyone else currently contracting with him.

I wish to create an online identity, post a reputational bond, and be trusted. My identity consists not only of a public key but also of a transactional protocol—a set of rules associated with that identity and its reputation, specifying how people are to deal with me. The protocol is designed to enforce transparency.

For a simple example, let the protocol specify that all transactions become binding only when posted to a particular web page, publicly accessible. That way, anyone transacting with me can see how many other transactions I am engaged in and whatever relevant features of the transaction—the size of a loan, say—are specified in the protocol.

**Reputation: Version Two**

In the discussion so far, “reputation” meant “reputation for fulfilling your contracts.” But there is another sort of reputation that is important in realspace—a reputation for competence in the activity you are performing for pay. When you hire a lawyer or a heart surgeon, it isn’t enough to know
that he is honest. That sort of reputation can also be established in cyberspace—and there too, the special circumstances of cyberspace raise problems, but problems that have their parallel in realspace.

Suppose I claim to be an expert in predicting real world events that potential customers wish predicted—the weather, the outcome of a particular legal case, the performance of a stock. Just as in realspace, I can establish a track record by making a series of correct predictions. There is, however, a problem.

To see it, imagine that my claim is to be able to predict, with certainty, the outcome of coin tosses—which many potential customers want predicted. Some people have that ability but, unfortunately, I do not. I proceed as follows:

1. I obtain a list of 10,000 potential customers.

2. I create 128 identities, each of which claims to be an expert predictor of coin flips, and divide the potential customers among them.

3. The first time a flip is to be predicted, half my identities predict heads, half predict tails. The coin is flipped and comes up heads. I scrap all of the identities that predicted tails and remove their customers from my current list—retaining their names and email addresses for future iterations of my business plan.

4. I repeat the previous step six more times.

I now have one surviving identity with about forty customers. Each of them has seen that identity predict a coin flip correctly seven times in a row, an event that could happen by chance less than one time in a hundred. Predicting coin flips is valuable, so each should be willing to pay a sizable sum for the next prediction.

I have just described the cyberspace equivalent of the market for investment newsletters or mutual funds. The chief difference—leaving aside the simplification of my coin flipping model—is that in my version the multiple identities all belong to the same person, making the fraud a deliberate one. In the realspace case, the publishers of each investment newsletter or the administrators of each mutual fund may actually believe that they know what the market will do next—and, each time, about half of them are right.

How might someone who really did know how to predict coin flips distinguish himself from those who did not but who might attempt to simulate that ability as described? The obvious answer is again some form of bond. When I first go into business making (public) predictions of coin flips, I also donate $100 in e-cash to some popular charity that is willing to
testify to the receipt of the money from my online identity. I then make seven consecutive correct public predictions.

A hundred dollars is not very much money. But in order to follow the business plan described in steps 1-4 above, I needed 128 identities—which, at $100 per identity, gets expensive. Furthermore, in addition to selling my prediction of flip number eight to paying customers, I also post it on my web page—after the customers have gotten their bets down but five minutes before the coin is flipped. After another ten correct calls, a potential customer can calculate that either I know something, or I am fantastically lucky, or I am the sole survivor of a collection of identities that cost somewhat over twelve million dollars to create. The generalization to someone selling investment advice, legal advice or medical advice online is left as an exercise for the reader.

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 cyberspace transactions.

REFERENCES


Bodde, Derk and Morris, Clarence, Law in Imperial China, Harvard University Press 1967.


Margoliouth, D.S. (tr), The Table-Talk of a Mesopotamian Judge, by al-Muhassin ibn Ali al-Tanukhi, Royal Asiatic Society (1922).
Siegler, Marc, Earthweb, (Baen Books: 1999).