Christina Ramberg*
Contracting on the Internet – Trends and Challenges for Law

1 Anonymity versus community

In the childhood of the Internet, many anticipated an open cyberspace where anybody could participate and no one would know who was acting at the other end of the line. Cyberspace was furthermore thought to be a lawless Paradise where no legislator or national state could reach out to regulate or punish certain behaviour. In an open environment it is technically complicated to ascertain the identity of senders and receivers of electronic messages. And without identity there is no incentive to behave honestly, since dishonesty cannot be pinned on a person deserving of punishment. Many feared that the Internet would become a lawless inferno and that doing business on a basis of honesty and trustworthiness would be impossible as long as there were no means of identification and no authority of law.

However, we have not seen either the lawless Paradise or the lawless inferno emerging on the Internet. Actually, what is now happening in cyberspace is not dramatic at all – but instead very similar to what we see in the traditional physical world ('cyberspace unplugged'): We see closed communities where deals are concluded between people who know and trust each other. Not everyone is allowed to participate in these communities. And misbehaving participants are severely punished by blacklisting and/or exclusion from further participation. What I mainly have in mind are closed B2B marketplaces where buyers and sellers in certain products meet to conclude a deal.

Another feature of the Internet of today is that, instead of being lawless, it is overloaded with law. Now every national state claims to have jurisdiction over everything that occurs in cyberspace. The national state has proven surprisingly successful in enforcing its regulations against Internet activities concerning its national interests. National states have also been very keen to regulate activities on the Internet.

In the following I will describe how legislators have responded to these trends on the Internet. I will also try to identify the lessons to be learned from attempts hitherto at regulating e-commerce.

2 The threat of anonymity

The fact that persons may act anonymously on the Internet is extremely frustrating from a legal point of view. We may pass thousands of legislative acts stating that promises should be kept, that we are not allowed to lie about each other and that we must not defraud others, but law serves no purpose if there is no practical way of tracking down the law-breakers.

Everybody knows that law is not the best guarantor of obedience to the norms of society. Instead the most important tool is social pressure. The risk of being branded as

---

* *Christina Ramberg* is a member of the IT Law Observatory. See presentation in Annex 1.

untrustworthy by family, friends and business partners is far more effective than any legislation. Our society has gradually become larger and more complex. The expansion of markets has made it increasingly difficult to ascertain the trustworthiness of potential business partners. This, in turn, has made law an increasingly important supplement to social pressure. When we enter into transactions with people whom we do not know and whose reputation is unfamiliar, we trust that they will behave honestly since they do not wish to take the risk of being punished by legal sanctions.

If on the Internet we do not know whom we are dealing with and we cannot establish their identity after a deal is made, after a promise is broken, after a lie has been put about, or after we have been defrauded, neither social pressure nor the law will serve as a means of preventing dishonest behaviour. This is indeed a great challenge to law. How can we preserve honesty in a cyberspace where anonymity flourishes?

As a response to this anxiety, the technology of digital signatures came as The Perfect Solution. Digital signatures based on the concept of Public Key Infrastructure (PKI) make it possible to create electronic identification. With the help of a certificate issued by a third party – i.e. someone other than the person who needs to establish someone else's identity – the identity of the sender of an electronic message can be ascertained. The level of security varies, depending on the technology used, the security routines of the third party or its subcontractors and – most importantly – the means whereby the third party initially identifies the certificate holder. In short, the party needing to identify the sender of an electronic message can choose to rely, not on the sender himself, but instead on a third party certifying the sender's identity. Some five or ten years ago many believed that PKI digital signatures would solve the fundamental problem of lack of trust in cyberspace and provide a necessary infrastructure for commercial transactions on the Internet. But it has turned out that digital signatures are not in high demand.

There are many reasons why digital signatures are not widely used. *First*, it has turned out that electronic transactions are not made in the open cyberspace between total strangers. Instead most transactions are made in closed communities where the parties' trustworthiness is a requirement for access and where the parties have 'met' before and by contract decided how to make future transactions. In such communities there is less need to put trust in a third party that issues certificates and less need for extremely secure identification methods. *Second*, digital signatures are cumbersome to implement since they require that third parties be recognised widely by the users, which has turned out to be quite complicated to achieve in practice. *Third*, to establish a high level of security with PKI is costly and there are other less secure – but secure enough – methods that can be used in closed communities and are less costly. In closed communities, the high and costly security that the PKI technology provides is not always necessary.

3 How law responds to the threat of anonymity

The legislators' response to the threat of anonymity is interesting to study. Quite early on in Sweden (in 1996) the Ministry of Justice held a hearing and asked business to what extent legislation was needed in relation to digital signatures. Not many found it worthwhile to attend this hearing. The representative of the International Chamber of Commerce strongly argued against legislation and claimed that the market forces would evolve slowly and that it was crucial to preserve flexibility. He said that legislation most likely would prevent development instead of helping business. The persons present at the hearing who argued that legislation was needed were mostly technical experts representing the digital signature industry. They argued that people were unfamiliar with the idea of electronic signatures and

would not dare to engage in electronic transactions unless the legislator explicitly stated that such transactions were legally valid and had sufficient evidentiary value. At that point the Swedish Ministry of Justice decided that Sweden need not take any legislative initiatives within the area of electronic signatures. In my opinion this was a wise decision, although I must admit that at the time I was surprised that business outside the digital signature industry did not ask for the legislator's help.

Internationally the approach was different. UNCITRAL (the United Nations Commission on International Trade Law) embarked on a new project in 1997 relating to digital signatures. That work was initially much inspired by the already enacted Digital Signature Act in Utah and the proposed legislation on digital signatures in Germany. There was a heated discussion at the first meeting as to whether legislation on digital signatures was needed and the importance was emphasised of not favouring one technical solution at the expense of others. The US delegation strongly questioned whether any regulation was needed. Since the same delegation at an earlier meeting had spoken in favour of regulating digital signatures, this intervention caused some confusion. The UNCITRAL negotiations lasted for four years, and the Model Law on Electronic Signatures was adopted in 2001. Throughout the negotiations the necessity and purpose of the Model Law remained a moot point. There was a constant struggle concerning the extent to which the rules should be technologically and media neutral. The influence from the industry representing certain types of technology (mainly PKI) was very strong. Another discomfort in the negotiations was the slowly emerging awareness among the delegations that the vision of the open anonymous Internet was not coming true with respect to electronic commerce.

On the European Union level there was great eagerness to show that actions were being taken to facilitate electronic commerce. It was thought that the way to facilitate for electronic commerce was by quickly enacting directives. The European Union would then be promoting legal certainty and harmonised law within the Common Market. It should come as no surprise to learn that the directives on electronic signatures and e-commerce achieved the exact opposite: legal uncertainty with respect to the legal effects of electronic signatures, disharmony within the Member States since the implementation of the ambiguous directives differs from one Member State to another, and obstacles to technological development and business flexibility, since the directive on electronic signatures indirectly favours a particular technological solution (PKI).

4 The threat of closed communities

As described above, the anonymity of Internet transactions posed a fundamental threat to society and it was feared that commercial dealings and trade would become impossible in the new electronic medium. However, the markets themselves circumvented this threat. Instead of using high security PKI technique for identification among strangers, markets developed closed communities where it was possible to establish the trust among participants that is necessary for commercial dealings. This initially unexpected development also poses threats, but of a less fundamental nature than the threat of anonymity:

a) When commerce is carried out in closed communities there is always a risk of the market forces becoming distorted. If not all potential buyers and sellers are allowed to participate in a market, competition may become inefficient. As we all know, the importance of competition and anti-trust law has increased considerably in recent decades, due to the idea that efficient competition is crucial for societies based on a market economy.

b) There are concerns that closed communities may become so dominant within their sphere of commerce, that they abuse their dominant position against participants in the marketplace.

c) Also within the individual closed community, efficient competition may be distorted by participants manipulating the price-setting mechanism by forming auction rings or by other collusive behaviour.

d) Another threat of closed communities is the single individual's inability to conduct business in a situation where he is not allowed access or is expelled from the closed community. The increasing use of different black-listing and white-listing schemes may severely damage the reputation of individual persons and businesses and in effect prevent them from engaging in Internet transactions.

The problem of anonymity on the Internet is to a great extent solved by the closed communities. At the same time, they entail negative implications mainly with respect to questions of efficient competition.

5 How law responds to the threats of closed communities

Legislators have been much less eager to take action against the threats of closed communities as compared to the threats of anonymity. This is not surprising. The threat of anonymity is aimed at the very foundations of society, whereas the threats of closed communities are less severe. Traditional law is fairly well suited to deal with the problems that closed communities entail. There are examples from German and US competition authorities where the transactions carried out in closed Internet marketplaces have been examined from an anti-trust law point of view. But we have not seen any initiatives to specifically regulate the risk of anti-competitive elements in Internet marketplaces as opposed to traditional physical marketplaces. Competition law is media-neutral and thought best kept that way. The challenge for competition law is to harmonise worldwide in order to avoid the problems of determining the law applicable to activities carried out in non-physical marketplaces and ensuring that that law is enforceable.

Many of the other legal difficulties in relation to activities in closed communities are best solved by the marketplace itself by contractual regulation in the Membership Terms and Conditions of Sale. There still remain areas where national law may create obstacles – such as requirements of licensing or form for auctions, and approval by authorities for certain types of transactions. Another problematic area is mandatory national consumer protection law and its differences between different states, for example as regards the extent to which a consumer is entitled to cancel a deal made by electronic auction. These examples, however, are of minor importance, and will hopefully be sorted out by the slow but inevitable process of gradual harmonisation of law. These are problems which are likely to be solved, not by new legislative efforts, but rather by minor amendments to the existing national law.

6 The lessons to be learned

6.1 Be reactive – not proactive!

It was already observed by Aristotle and has been repeated many times since, that a sovereign's possibility of influencing citizens' behaviour by legislation is very limited. This is particularly so in the field of private law. The role of legislation in that area is mainly to codify already existing conduct – not to proactively steer behaviour in certain directions. There was, understandably, great concern that the threat of anonymity would make commercial dealings in cyberspace impossible. However, the legislators' initial attempts did electronic commerce more harm than good. Eagerness to establish legal certainty – to assure the markets that electronic transactions were legally valid – led to favouritism of a particular technology (PKI). The legislator gave the misleading impression that for a transaction to be legally valid it had to be effected by PKI technique. And since business was not prepared to pay for the excessive security and cumbersome administration that this technology entailed, the development of e-commerce actually became slower than necessary.

The legislative experiment in relation to electronic signatures has taught us a lesson. It is better to be reactive than proactive within areas that have not yet matured with respect to business models, usages, technology and actual practical problems. I agree with the initial approach taken by the Swedish Ministry of Justice: Let us wait and see if there is any real need for regulating electronic signatures. Let us wait and see if any particular problems or abuse arise before we take legislative action. Let us trust that the general law is able to handle the most urgent and most fundamental issues. If we see a need for particular regulation, we will be able to do something about it in due course. The legislator should not take the lead and try to steer development. It is better to be reactive and take action when there is a real existing problem, than to be proactive and try to foresee the possible problems and regulate before they have come into existence. A proactive legislator may do more harm than good by misleading the citizens to believe that there is Only One Single Solution to a problem that may be solved more efficiently in other ways than the one suggested and regulated by the legislator.

The fundamental issue of trust in a marketplace can be resolved in many ways. It was initially believed that the only way to create trust was to enact legislation on electronic signatures. In the event, however, the markets found other means of establishing trust and confidence. The lesson to be learned from this experience it that the role of legislation is not to create trust, but merely to support already existing trust.

It is my hope that the present fallacy among businessmen that the PKI technique is essential in order to create legally valid contracts, will soon fade away. I am, however, concerned that this may take many years and in the meantime cause unnecessary investments in a costly infrastructure, as well as slowing down the development of e-commerce.

6.2 Be media neutral!

Another lesson to be learned is that the problems in contract law are eternal and exist independently of the medium used to perform the transactions. The eternal problems are, among others, when and how a contract is formed, and the liability for fraud, mistake and delayed or defective performance. It is not wise to regulate these issues specifically for electronic transactions, since the problems occur in all types of medium used. In the future, it will be almost impossible to distinguish between transactions made by electronic means of communication and others. Transactions will to a large extent be a mixture of electronic and non-electronic communication. It would be devastating to have legal regimes addressing the same problem differently, depending on what medium was used to conclude a deal.

6.3 Harmonise law internationally!

The third lesson to be learned is that cyberspace is not a lawless inferno or Paradise. At present cyberspace is overloaded with law – which most persons associate more closely with Hell than with Paradise. All national states claim to have jurisdiction at the same time and in parallel in cyberspace. The solution to this problem is to harmonise law worldwide. It makes me very optimistic to see how greatly the efforts and success of international harmonisation of contract law have increased during the past decade. Electronic contracting on the Internet has helped to speed up this development of harmonisation and is likely to go on doing so.