THE NETWORK SOCIETY: A PROPOSAL FOR A STATELESS SOCIETY

Abstract. I present a proposal for a libertarian society based on a network containing the rules accepted by the members. Various questions are considered: the implementation of network software, the development toward a libertarian society in a statist environment, the dangers related with natural monopolies, the very foundations of libertarian ethics.

Contents

1. Introduction

I'm libertarian. The state is, in my opinion, a criminal gang, worse and more dangerous than any other gangs. The aim of this paper is not to justify this position – it is sufficiently justified in a lot of other libertarian writings. I can summarize my rejection of the state in a single sentence: The state openly violates one of the most important ethical principles at all, if not the most important one – the Golden Rule. What could be worse?

And I think we have a chance to get rid of it, that a society without state is a realistic possibility in our modern world. But how?

My answer is the main content of this paper. I do not cover everything. For example, I do not consider the problem of defense, in particular military defense against states. See [1, 2] about this.

What I propose to develop a libertarian network. Its members present in this network the rules which they accept for themself, together with a list of arbiters they accept as fair. If someone else thinks that you have violated your own rules he can ask these arbiters to decide about this. Violations of the own rules, as established by the own arbiters, will be published in a global black list, with open access to everybody.

The network gives immediate advantages for its members: They can find there similar-minded people to cooperate with. They obtain some information about their reliability. One can make contracts with other network members which would not be supported by state courts. Nonetheless, one can be sufficiently certain that the contract will be fulfilled – the black list will be sufficient to enforce this.

An important advantage is that the network can be created and developed already in a world full of states. The new, libertarian society can show how it works, and that it works better, without destruction of the existing, working society. This minimizes the risks related with the creation of a new society. If the network doesn't work at all, nothing wrong happens: No Gulags, no killing fields, nothing, except that some people have participated in some strange network game and given it up after some time.

And if it works only partially, so that it appears that some things can be managed in the network, but some others, like the army, have to be left to states, there is

no problem too. The full libertarian dream would not be realized, but the society would be improved, would be much more libertarian than today.

In any way, the network provides a peaceful method of transition into a more libertarian, possibly even completely libertarian society. Everybody is free to participate in the network or not. Everybody is free to decide which rules he accepts in the network – these rules may be, in particular, also the laws of some state one considers to be just. Nobody is forced to give up the state. Of course, the libertarian members of the network don't accept the laws of the remaining states as ethically relevant and feel free to violate them if possible and not too dangerous. But this will be as peaceful a revolution as those of 1989-1990, where people have peacefully violated laws of the communist states too.

Different from Marxists, I'm happy to work out the details of my proposals. So they may be criticized in detail. If the proposal is utopian or otherwise unrealistic, this can be detected already in pure theory. So my network proposal is open to criticism. If it appears faulty, indefensible, it would be even unnecessary to implement the network software and to start the network. The aim of most of this essay is to work out the network proposal in some detail. There are a lot of questions which have to be considered.

In particular, to be able to manage all the rules of all the people on Earth, one needs appropriate, sufficiently fast software. To handle pure text would be impossible without a lot of artificial intelligence. But there are much simpler possibilities. In particular, one can use some sort of standardization of the rules. This sounds dangerously restrictive, but it appears much less restrictive as it seems. Nonetheless, it is important to think about ways to manage this standardization in such a way that it restricts the freedom of choice of the own rules only in a minimal way. Then, how can property claims be managed in the network? One also has to think about simple automatic algorithms for the evaluation of the reliability of others.

There are other things to think about. The network suggests an interesting subdivision of ethical questions. On the one hand, there is the question of honesty, of fulfilling the own promises, of following the own rules. On the other hand, the there is the content of these rules and promises, which may be quite amoral, up to the extremal case of contract killers. The black list of the network covers *only* violators of the first kind – those who break the own promises. There appear some foundational questions: Is this ethically justified? I give a positive answer from point of view of rational self-interest: Somebody who violates his promises cannot be trusted. If you don't like the rules of somebody else, but if he holds his promises, cooperation is possible.

This leads into another domain of inquiry – the very foundations of libertarian ethics. I present here my own approach, and this approach in fact reflects this subdivision too. It seems useful to distinguish two different domains of ethical theory. First, a theory of honesty, which considers only the single ethical value of honesty, of fulfilling given promises. And, second, a theory about the content of such rules and promises. These two parts are indeed quite different. The main questions have almost no connection with each other.

The main problem of the theory of honesty is why it is reasonable to be honest in general, if there are situations where honesty becomes irrational, and how to handle these situations. The very foundational questions of ethics of type "why should we follow ethical rules" appear already in this part, exemplified by the question "why

should we fulfill our promises". The question what are the ethical values has, in this part, an easy answer: There is only one ethical value considered here, honesty. And the network is quite sure about this part too: Those who violate this value, those who break their own promises, appear on the black list.

Instead, in the part about the content of the rules we do not have to care anymore about these foundational questions. Once I'm honest, and once I have accepted some rule, the problem is solved – I have to follow it. The question is now a pragmatical one: What are the rules which a rational human being would openly accept for himself? The network is completely open about this question, does not lead to any preference for one or another solution.

Nonetheless, I propose here also some ideas. First of all, the key ethical rule, which distinguishes the libertarian from the proponents of a state, should be the Golden Rule. It forbids legal monopolies and, therefore, the state. This seems much better than a non-aggression rule, which depends on a lot of details necessary to distinguish justified self-defense from aggression. The Golden Rule is, instead, a simple and clear symmetry rule, and it can be easily and unquestionable established if a set of rules is in agreement with the Golden Rule.

But the Golden Rule covers only some part of the rules – general rules, which restrict only really dangerous behaviour. Other ethical rules, like prescriptions of particular religions, vegetarianism and so on, are better handled as additional promises, independent of the Golden Rule. On the other hand, property claims can be considered as exceptions from the Golden Rule too – they are claims of monopoly rights over the property.

This leads to another natural subdivision – the subdivision into property claims and their acceptance by others. It seems reasonable to incorporate a management of property claims into the network. But, different from similar institutions of states, it is not the job of this management to make decisions about the just owner. There will be quite different ideas about which property claims are justified or not. The network management system will contain only the information about property claims themself and what has been proposed to justify them.

Such a system of property management seems heavily prejudiced in favour of the pro-capitalistic direction of libertarianism. But in fact this question is undecided. Anarcho-communists may as well accept and follow the Golden Rule. I think this is an important advantage of using the Golden Rule as the ethical foundation of a libertarian movement. There is no reason to exclude those communists from such a movement who are ready to accept the Golden Rule.

In fact this should be one of the central points of a libertarian movement – that it is open for very different ideas of organizing life. Communism is economically inefficient, but so what – this is not yet a reason to treat anarcho-communists as enemies. Anarcho-communist communes can have their fair place in a liberarian society, as long as they don't start to use violence against those who do not share their communist views. There are, of course, strong reasons to suspect that anarcho-communists are not really anarchists, but, instead, only hidden communists. But the network helps to decide this question. To participate, the anarcho-communists would have to put their own rules into the network, so that we can see and evaluate them.

Last but not least, one has to think about defense against the state. One can expect that etatists will not like such a network. Moreover, it is reasonable to

expect that the participants will use the network for various illegal activities. This is, last but not least, one of the advantages of using the network – if one wants to "perpetrate" victimless "crimes", the network is a fine place to find similar-minded people to cooperate. Even more, once the network becomes large enough, one can expect that an internal banking system develops. This banking system will be out of control of the state, which makes it attractive for money laundering and tax evasion. From libertarian point of view, nothing of this is problematic: Victimless crimes should be decriminalized, and the statist control of the banking system is extremely dangerous for freedom.

But the states have a different opinion about this, and therefore one has to expect heavy attacks from the state. What can one do to defend the network? First, there are good arguments for legality. The basic activities of the network should be legal in a democracy: One cannot forbid the people to tell openly about which rules they consider to be just. One cannot forbid people to promise to follow their own preferred rules, except for a few exceptions where it is promised to break laws. It seems hard to forbid freely chosen arbiters to tell everybody about their opinion about a particular event. And it seems also hard to forbid to publish these opinions, given that they are made about people who have agreed that the opinion of the arbiter may be published there. One would have to forbid the distribution of opinions. In other words, the state would have to become quite totalitarian to forbid the network.

Given the arguments in favour of a legal network, the network members can try to fight a law which makes the network illegal by Ghandi-like methods of open, demonstrative violation of these laws.

Then, the possibilities of the network will be especially interesting for the rich, powerful, and intelligent, or, in other words, for the elite. So there may be a lot of defenders of the network inside the ruling class. The common interest of the ruling class in the preservation of the state is only a common good, their particular gains from using the network are, instead, private goods, so that they may care more about the network than about the state.

Of course, this does not make sure that the state will not fight. What to do in this case? First, there will be some technical and organizational methods to avoid persecution. In particular, there will be pseudonymous accounts, and the decision of which information one puts into the network has to be completely left to the individual. The techniques for anonymous networking have been already implemented in networks like Tor and freenet. If the use of particular software will be forbidden, one can implement this software as a "friendly virus" – a program which is indistinguishable from a virus and behaves like a virus if one does not know how to use it, but can be used in a safe way if one knows how. The behaviour of an infected program can be made indistinguishable from the use of the program. So, or the state incarcerates all those infected by the virus, or it becomes impossible to prevent the use of the program.

Whatever the possible defense methods, the state has possibilities to win: In a totalitarian state, where internet is forbidden, the network cannot survive. But the costs will be high. Not only for the personal freedom of the citizens, but also in terms of comfort and productivity. If the network is prepared to meet this challenge, a small increase of repression will not be dangerous at all. This will be a good argument against them in a democratic discussion. If it becomes clear

that the etatists can win only if they go the full way and, in particular, have to shut down the internet, one can hope that they will not even try. Or, if they do, not everywhere. Then, the economic progress of those regions where the network remains legal will decide the fight.

If the network remains legal, it will be almost impossible to prevent the increase of the membership until almost everybody is a member. Indeed, the network gives safe possibilities to participate in illegal markets, so everybody with *some* illegal interest will participate. Given the increasing control of everything by the state, these will be quite a lot of people. Then, everybody interested in safe contracts with other countries will prefer arbitrage in the network in comparison with an unknown system of law enforcement of other countries. Then, there are already a lot of things in contracts which cannot be enforced in state courts. If people want to use such contracts in a safe way, they will use the network, even if the legal unenforcable part is quite harmless. Last but not least, with a sufficient large number of members and a corresponding large internal circulation, the internal banking system gives everybody a powerful method of tax evasion. An untaxable shadow economy may develop.

On the other hand, it is worth to think about cooperation between the network and the state too: The state may become a member of the network himself. This leads to an improvement of the state in a quite natural way – the states which participate in the network, as well as the political parties of these states, have to compete for reputation in the same way as ordinary people, with the same criteria. This may have a civilizing influence on the state – its criminal character may decrease.

Thus, there are a lot of questions to think about. Let's start.

2. The basic idea of the network

Let's start with the basic idea – the idea that everybody defines his own set of rules and penalties for violating them as just, accepts an own set of arbiters as fair, and those who refuse to accept the decisions of their own freely chosen arbiters will be published in a black list visible to everybody.

2.1. **The problem of the stranger.**

In a small society, no state is necessary. The reason is simple – everybody knows everybody. If you break your promise, the victim will tell everybody about it, and, as a consequence, nobody will believe your promises in future. So, to hold promises is almost obligatory – one cannot break them regularly, repeatedly. The natural penalty for breaking a promise – non-cooperation by others who do not believe the promise-breaker – is sufficient to enforce promises in such a small society. It is unavoidable: The victim will tell everybody about the fact, and everybody is eager to learn about such things out of his own self-interest. And you will be penalized for breaking the promise not because of some official moral obligation, but out of simple self-interest: Other people are afraid of cooperation with promise-breakers because it is risky to cooperate with them.

Because of the unavoidable penalty for breaking a promise, it becomes stupid to break them. As a consequence, it seldom happens. So, it is reasonable to trust others. As a consequence, in the rare cases where it happens, the penalty will be even more rigorous: First, promise-breakers are rare exceptions, and, second, the

difference between usual behaviour – trust – and non-cooperation will be larger. And it becomes even more reasonable to hold promises.

Unfortunately this changes if small villages become large towns. It is no longer possible to know everybody, at least not in sufficient detail. So, a problem appears – the problem of cooperation with a stranger. You don't know him, you don't know if he holds his promises or not. And if he breaks his promise, you will be unable to tell his future victims about this, for the same reason his earlier victims have not told you about him – you don't know each other.

So it is no longer rational not to break promises. The penalty for breaking them decreases with the size of the town. In a large enough town you can make a living by breaking promises repeatedly. All you have to do is to find new victims.

But, once you cannot exclude this, there will be much less trust in general. As a consequence, the effective penalty for breaking promises decreases – once there is not much trust anyway, there is not that much to loose. And so it becomes even more reasonable to break promises. Therefore, more promises will be broken, and it becomes even more stupid to trust others.

One solution of the problem is that of small networks of trust – you can trust your family, and a few people in your environment, but only after a long time. But you cannot trust strangers. So this solution only prevents a complete breakdown of cooperation. It does not solve the problem of cooperation with strangers.

The other classical solution is the state. Instead of trusting the stranger, it is sufficient to trust the police. If the stranger violates the common law, you call the police, and the police will help you and enforce the law – force him to fulfill the contract.

This solution is also not optimal. In particular, it remains rational to break promises if the police is unable to catch you, or your victim is unable, for whatever reason, to call the police. The typical case of the last situation is a victim who has violated some law himself, and to call the police would be too dangerous for the victim itself.

But today a new solution is possible – a network. Information about somebody who violates his promises you can give, today, to the whole world. Thus, if this is organized in an appropriate way, the solution provided by the state becomes as unnecessary as in a small society. This paper is about the question how to organize this. The resulting solution is, again, better than the police solution – it becomes, again, rational to hold your promises, as in a small society.

2.2. **The human right of separation.** If the state is considered as a useful organization for its citizens, the right of a group of people to separate, to create their own, independent state, would be a natural right. The denial of the right of separation shows, in a simple and obvious way, that the state is an instrument of exploitation. People or groups of people who do not want to participate, but, instead, want to organize a separate state, are forced to remain in the state. This obviously cannot be justified by the harm done by the separating group – all the separating group wants to do is to establish an own state. If this would be wrong, the point that states are inherently wrong would have to be admitted. So, to forbid separation is clearly unjust.

So, if one wants to defend the very idea of the state as just, one has to accept the right of separation for every group of people who likes it.

In particular, this argumentation does not contain any lower bound for the number of people who wants to separate. So, this number can be as small as one likes. In particular, it may be as small as one. So, everybody should be free to separate from his state and to create an own state, and, in particular, to establish his own laws.

But even those who accept the right of separation for large populations often do not accept the right of individuals to separate. And there is even an argument which can be used to justify this position. The argument is that separation of a single person would violate the Golden Rule, because one cannot wish that everybody uses this right. Indeed, the consequence would be a world where everybody has his own set of laws. A world with more than 6 000 000 000 different complete sets of laws. It is hard enough for international trade to live in a world with a few hundred of different laws – a single world law would be much simpler and preferable – but this is something we have to accept up to now.

So a world with more than 6 000 000 000 different complete sets of laws would be unmanagable even in principle.

But, sorry, I disagree. This problem can be solved. The simple solution is standardization. We will consider the details in section 7. The standard fixes the text of the articles, but leaves you the complete freedom of choice about the numbers, in particular, the penalties. So, if you think something should be legalized, simply put a number 0 for the penalty. The standard will be established by free competition between those who like to propose such standards. Once all the differences between different laws using the same standard are only numbers, one can use simple and fast programs to compare them.

2.3. **Who is obliged to follow all these laws?** The next trivial objection is the question who is obliged to follow all these laws. The answer is a quite trivial one: Once you propose these laws as just, you are morally obliged to follow them. You and nobody else. You propose the rules for your own behaviour. And you, and only you, are obliged to follow them.

But, in this case, why would one accept such laws at all? Very simple, for the same reason why you accept obligations if you sign contracts. You are interested in cooperation with other people. But in a libertarian society nobody is obliged to help you, no state gives you any social support, so that you depend on the cooperation of other people. And other people will accept you as a possible partner only if you promise to follow reasonable rules. So those who accept reasonable rules have an advantage: They will be preferred as partners in cooperation.

Remember that the network is designed in such a way that people can use automatic search for those with the best rules. If you want to sell something on the net, you make proposals about your prices in the net. The lower the price, the greater the probability that you find somebody who wants to buy it. In the same way, if you want to cooperate with others, and make proposals for this on the net, your rules will be part of this proposal, and therefore it depends on your rules if you will be accepted as a partner or not. The more restrictive your rules are for you, and the more you allow others to do, the greater the probability that other people will agree to cooperate with you.

Now, if we start the network in our current statist society, these rules are simply some additional restrictions for you. The laws of the state do not disappear yet. If you violate these laws, you will be punished as usual by the state.

But your rules will have an influence. People will distinguish between those who violate only some law which they openly consider as unjust and those who violate their own rules. Those of the first group will be considered as something like political prisoners – people who fight for a different set of laws. One may disagree with them, but one can nonetheless trust them. Instead, those who break their own rules will be considered as real criminals – people who do not deserve any trust.

2.4. **Who controls this?** But who decides if you follow your own rules or not?

The idea is simple – you also define a list of arbiters. Arbiters who, in your opinion, are fair and trustworthy. If one thinks that you have violated one of your own rules, broken your promises, one can ask one of these arbiters to decide about this. Then the arbiter decides. If you have violated your own rules, you have to accept the penalty described by your rules.

Here, a question similar to that of the rules appears. What if I am far too restrictive in my choice of arbiters? The simplest idea would be to accept only myself as an arbiter. It would be not much better if I accept only a few of my best friends.

In principle, this is allowed. There are no restrictions – everybody can work as an arbiter, no qualification is necessary.

But, of course, if you accept only your best friends as arbiters, nobody will trust you. You can obtain trust only if you accept arbiters who are accepted as fair by many others, at least by those you would like to cooperate with. Of course, this also increases your risk of becoming a victim of an unjust arbiter. But the very principle is clear – to find people who are ready to trust you, you have to accept widely accepted, neutral arbiters.

And, once you have understood that it is reasonable to accept sufficiently restrictive rules, you will also understand that it is reasonable to accept sufficiently fair, neutral arbiters instead of your best friends. Last but not least, the risk is not that big – the worst thing you can suffer are penalties which you have accepted as just.

2.5. **The black list.** But what if you don't care about the decisions of these arbiters, if you simply don't pay the fine or run away? In this case, there is another form of penalty – a global black list.

Technically, there is no problem to arrange such a black list in a safe way: You have accepted the arbiters as just, and this acceptance has your electronic signature. The information on the black list is electronically signed by the arbiter. Thus, every entry in the black list has to contain these two signatures – your own that you accept the arbiter, and that of the arbiter about his decision. Any program can check this automatically. There is no great danger that such entries will be faked: Electronic signatures are much safer than signatures in the real world.

Of course, the black list is open for everybody to check. So everybody else will know, forever, what you have done, that you have broken your own promises. And one can predict the reasonable reaction – those who violate their own promises will have a hard job to find somebody ready to cooperate with them.

It does not mean that everybody is now obliged to punish or boycott you. Not at all. It is the free decision of every participant how to react. He may ignore the information. He may even use the available information about the dates to

ignore the information automatically – because it was too long ago, because it was a beginners error, or because you have been too young. The date of the decision will be known in any case. If other relevant dates, like the date of your entry into the network, your date of birth, or the date when you have violated the rule, are known or not depends on your private decision. If they are, fine. If not, this will probably not used in your favour. Other things, like the seriousness of the violation, will be harder to evaluate automatically. But if you use rules with a penalty, so that you appear on the black list only if you don't accept the penalty, the penalty is a good information about this.

The decision about forgiving a promise breaker remains a free individual decision. No pressure of the society as a whole is necessary to enforce a modification in one or another direction. It is simply risky to cooperate with promise breakers, and this is sufficient to reduce the number of people ready to cooperate with them. But how risky it is depends on many factors. Everybody is free to evaluate them himself. Last but not least, if you are the only one who is ready to cooperate with such people this can be useful too. In their situation, they will be ready to give you much better conditions. They will be ready to work for much less money, to pay in advance, allow you to control a lot of things and so on. In other words, for the risk of cooperating with these people you will receive some return.

And, last but not least, there are also other people with records on the black list. They have not much choice among those without a record, so they will probably agree to cooperate with other word-breakers.

Because of this, it seems unlikely that people on the black list will be boycotted completely and forever and would have to starve to death. Nonetheless, a record on the black list will be a very serious penalty.

In the network society, everybody is free to use his own moral principles in his decision to forgive. One may think that every promise breaker should be banished forever. Another may think that every promise breaker deserves a second, third, or forth chance. Everybody decides himself – it is his own risk that the promise breaker will break his promises again.

2.6. **Pure and personal pseudonymous accounts.** It is the free decision of everybody which information about himself he wants to publish. The motivation for publishing private data at all is that an account which provides a lot of personal information will be trusted more than a pure pseudonymous account. On the other hand, personal information may be misused. So one has to think about the question what to publish and what to hide. We will distinguish here only the following three different types of accounts, even if there may be a lot of intermediate forms in dependence of which information is given:

- *Open accounts* provide open information about their real personal identity.
- *Personal pseudonymous accounts* provide information about their personal identity to the arbiters, so that it will be openly published in case that they appear on the black list. The arbiter confirms this, so everybody can distinguish them from the last type:
- *Pure pseudonymous accounts* provide no such information. I could have named them anonymous accounts, but they are in fact pseudonymous accounts in the usual meaning of the word – you can exchange information with it and be sure that it is always the same person you are communicating with, a person who is uniquely identified by the name of the account. So

they can also build a reputation for holding their promises. But it is less dangerous for them to break their promises – it is only the account which appears on the black list, not their real personal data.

In a libertarian society there will be not much reason to use pseudoymous accounts. The advantage of trust connected with an open account will be a sufficiently strong incentive to prefer to do everything with an open account.

On the other hand, even in a libertarian society one may prefer privacy. In fact, there will be, even in the most libertarian society, criminals too, people who like to misuse personal information. Once hiding personal information *can*, at least in principle, increase your security, there is a legitimate reason for using pseudonymous accounts even in a completely libertarian society.

Moreover, even in a very tolerant society there will be some public opinion, and it will have some power, and it will often err. But to argue against public opinion is always uncomfortable, it can decrease your reputation even if your opinion is correct. So people may prefer pseudonymous accounts to argue against public opinion. This is another legitimate reason: The correction of errors of public opinion is an important service for the society as a whole.

Nonetheless, it seems reasonable to expect that in a libertarian society open accounts will be the rule, and pseudonyms the exception.

The situation is quite different today, or in the initial phase of the development of the network. There are a lot of powerful criminal organizations around us named "states", organizations which are likely to misuse our personal data for such dangerous criminal activities like robbery (named "taxation") and violent aggression (named "enforcement of law"). In this situation, pseudonymous accounts are simply a necessity, and it is quite reasonable to expect that the situation will be reverse: Pseudonyms will be the rule, and open accounts the exception.

3. Arbitrage

We have already mentioned that in principle everybody can become an arbiter. All one needs are other people who trust you enough to accept you as their arbiter.

Of course, arbitrage is not without costs, so each arbiter will establish prices for his services and specifications of what will be done. All this is also open information.

If you think that somebody has violates his own rules, it is your decision, and your risk, to call the arbiter. In fact, if the decision is against you, it is quite probable that you have to pay the arbiter. So there is some risk. But the conditions are open, part of the rules of the arbiter, so you can estimate your risk.

As a consequence, the situation in arbitrage is quite different from the situation now: Above participants have to accept the arbiter as fair.

3.1. **Higher instances.** Arbiters sometimes err. One would like to have a possibility to correct such errors. No problem. Arbiters are participants of the network and therefore have their own rules. Once they work as arbiters, they will have some special rules regarding their job. These rules about their job will contain some rules about other, higher instances. In particular, if these rules contain a possibility of reconsideration in higher instances, there will be also such a list of arbiters accepted as such a higher instance.

What will be the rules of these higher instances? This depends on their own decisions. The higher arbiters are themself members of the network, thus, they

have rules themself, rules which they have accepted themself. In particular, they may accept a reconsideration of their own decisions in yet another instance, or they may not. But probably they will – without a possibility to correct even gross errors, who whill accept them? And so on.

Ad infinitum? Yes. There is no a priori upper bound for yet another instance. There will be, in particular, circles: You accept me as your arbiter, I accept you as my arbiter. If somebody does not like my decision, he call you. If he doesn't like you decision too, he can call me again. And so up to infinity.

In fact, this situation will be unavoidable. Everybody accepts somebody else as his arbiter. So let's start with you and make a list of the arbiters of the following instances. There will be no end of this list – everybody accepts somebody else as his arbiter. But there are only a finite number of different people on Earth. So, there will be some repetition, somebody will appear many times on our list. And that means we have identified a circle. And if there is such a circle, one can follow this circle ad infinitum.

But is this dangerous? In no way. The arbiters themself will be happy – they do some work, thus, receive some payment for this. In case of the circle, the work becomes simple – a repetition of the previous decision – thus, easy money.

But that means there will be no certainty about the final decision? Not at all. The default way will be different: The decision made by the first arbiter is what you have to live with. The next arbiter decides only if the first arbiter has violated his own rules. So, it is a decision about, possibly against, the arbiter. The penalty may include a reconsideration of the decision, or paying a fine to the victim of his unjust decision. But this depends on the rules of the arbiter.

In other words, how many instances can possibly change the very decision is something people have to decide themself: If there are too many instances, decision making takes too much time. If the number is too small, obviously wrong decisions cannot be corrected.

But there is also a quite reasonable idea for a compromise: One question is to chance the decision itself, but another one a compensation for the victim of an unjust decision. The first question may be decided in a final way in the first or second instance. So the winner will be certain about his victory very fast, and the loser has to live with this. But the victim of an unfair decision of a prior instance may be compensated in the next instance, with the penalty to be paid by the arbiter of the previous instance.

3.2. **Fake networks.** At least in principle, it is a danger in an electronic network that the same real person can create many different accounts. These accounts will pretend to be different people and support each other in various ways – in fact in all the ways in which real people can support each other in the network too. All this may look like a real subnetwork of really trustworthy persons.

As a consequence, the members of such faked subnetworks could look like higly trustworthy persons. In the best case, the aim is simply to obtain higher reputation without misusing it. But it is more probable that behind such a fake network is the intention to cheat. Especially dangerous is if such a network fakes also arbiters. In this case, those who have faked arbiters will never appear on the black list – their arbiters will always decide in their favour. The network has to take these possibilities into account.

Another danger which has to be taken into account are spam accounts or police spy accounts. The only more or less secure method to fight such fake networks and spam attacks seems a management of personal identification.

One can try to start them, by creating a lot of fake accounts filled with persons who claim to trust each other, some of them fake arbiters of every level. But if it doesn't have such a connection, and none of the fake arbiters ends up on your personal list of reliable arbiters, you will not trust anybody from the fake network. Those newbies who believe one of the fake arbiters will learn about their error in a single experience. So the subnetwork does not have a chance of establishing itself in the long run. Even newbies, who may simply start by copying a list of trustworthy arbiters from experienced members they personally trust, will not become regular victims.

On the other hand, the possibility to create such a fake network shows the necessity of some element of personal trust. Once the content of the fake network may be identical to that of a real subnetwork, no program which can access only the content of the network itself would be able to identify the fake network as a fake. It is only the connection via personal trust which allows to distinguish fakes from reality.

3.3. **Learning from experience.** One possibility to fight fake networks is the use of higher order arbitrage.

In a small network, you may personally trust a few arbiters, knowing them in real life, or learning that they are trustworthy from good friends who know them personally. This possibility decreases with the size of the network. But there is a replacement: Personal trust in higher order instances.

Of course, if the whole world participates, the number of arbiters will be large. And even second instance arbiters will be far too much. Nonetheless, one can continue the very idea and consider the third or forth instances. This will be already sufficient: If we are optimistic and think that each instance reduces the number of arbiters by a factor 1000, the third instance is sufficient to cover the whole world: It remains to trust personally 6 arbiters. If we are more pessimistic and assume a reduction factor of only 200, the $6 \cdot 10^9$ reduce to $3 \cdot 10^7$ simple arbiters, $1.5 \cdot 10^5$ of second order, $7.5 \cdot 10^2$ third order and 4 forth order arbiters. Are these reduction rates realistic? I don't know, but I think with arbiters trusted by above sides of a conflict the probability that the next instance will be called may be much lower than in state courts – courts not based on any personal trust by above participating sides.

Moreover, most conflicts happen between people living in the same neighbourhood. Here, personal knowing and trusting arbiters remains easy, even in the first instance.

Given this scheme, you can leave the work of establishing if there is a trustworthy arbiter to a program – all the program has to do is to find a connection from one of the arbiters of a given person to an arbiter of your personal trust such that the arbiter of your trust is accepted as the third- or forth-order instance for his decisions.

Following this scheme, you (and the network) have now a possibility to learn from experience. Whenever you feel cheated, there are only the following possibilities: Or you will be compensated for this in one or another instance – in this case, everything has been fine and there is no necessity to learn something. Or one

of your opponents ends on the black list – in this case, the whole network learns something new, and your program too, so that there will be no repetition of the error. Or you understand that you have misinterpreted one or another condition of the rules of those involved – in this case, you can learn from this personally, but you can as well modify your program so that it makes in future stronger requirements. Or the story ends with an unjust decision by an arbiter of your personal trust – and in this case, you will remove this trust. So if something goes wrong, you can always modify your program in such a way that the error – to trust somebody who does not deserve it – will not be repeated. Even better, in some cases the whole network becomes better informed and learns too.

As a consequence of this concept, completely isolated fake networks will not be trusted – they do not accept arbiters from outside, because this would be dangerous. But in this case, there will be no connection to some arbiter of your personal trust.

There are also possibilities to allow others to learn from your experience. For example, nobody forces you to hide your personal list of reliable arbiters. You can distribute it freely, so that other people can use it too. Then, your experience with particular rules is also something you can share in discussions with other people.

4. Ideologies in the network

Is there some natural connection between some ideology and the network? It seems, there is. Ideologies are nothing which appears without reason, without base in the real world. Instead, they fulfill some function. I do not want to defend here some trivial marxism that the ideology is predefined by the circumstances we live in: The influence of the circumstances we live in on our ideologies is only a tendency, and there is also a strong influence in the other direction, from our ideas on the circumstances we live in.

Nonetheless, the network will have some influence on the ideology of it's participants, and one can make some reasonable predictions about this influence based on the circumstances of life in the network.

The mechanism how the network can modify the ideology is simple: Initially, the network will be most attractive to some subset of people – those who find some of the differences between the network and the current society most attractive. These first users can be expected to support ideologies which consider the differences between the network and the current state as advantages of the network and highly value these advantages.

These first users are those who build the infrastructure of the network, occupy the best positions in the network, teach the next generation of newbies how to use it, and obtain almost automatically a high status as veterans of the network. All these three factors give their ideologies some strong advantage.

Instead, those with ideologies which consider the differences as disadvantages of the network, and the network itself as dangerous and evil, will be the last who will participate in it. Therefore, at least initially their influence on the network will be much weaker, and it becomes much harder for them to gain influence. (The only way for them to gain power is to find some problems which are handled badly by the network and the infrastructure created in the first phase – problems which have been ignored, because they have not been important for the first users.)

Thus, there are objective reasons which will favour some ideologies and disfavour others. It remains to find out which ideas will be favoured by the first users of the network.

4.1. **Revival of personal honour.** In most archaic societies, holding the own promises is much more important than today in modern democracies. This is not an accident, but a natural consequence of the problem of the stranger: Only in a small society it is possible to verify if somebody holds his promises – for a stranger, we have no way to verify this. Therefore, we have to rely, instead of his word, on general law and the police enforcing it.

But the network solves this problem. It becomes possible to evaluate the personal honour of a stranger, by evaluating his rules and the available information about him: If there is no record in the black list, and the arbitrators he accepts are reliable, it is reasonable to trust him.

As a consequence, the ideological value of honour and other personal qualities considered today in some sense as archaic will raise again.

4.2. **Self-determination as a central value.** While holding the own promise is an old, almost archaic value, which will revive in the network, there is another value which is quite modern: *self-determination*. Here, again, it is that the network makes self-determination possible in a domain where it has been impossible in the past – the domain of establishing the rules for the own behaviour. This is an obviously much more important point for self-determination than particular hobbies or fashion or the choice of the preferred music which is what is self-determination reduced to in democracy. If one has to follow rules defined by others, some government, one is not self-determined, but government-determined, and it does not matter at all if the government is monarchistic or democratic: Your participation in the election does not make it your government, it remains to be a government, which governs your behaviour because it establishes the rules you have to follow.

The meaning of self-determination in the network is therefore much stronger, contains much more than in democracy, where the most essential parts of self-determination are not given to the people. So one can also expect that self-determination, in this strong meaning of the word, will be an important value for the participants of the network.

4.3. **Acceptance of the natural consequences of your own decisions.** Part of the self-determination in the network is that one cannot cry for government support if one has made a bad contract. One is, of course, not obliged by any state laws to follow a promise not to call the police, but then the record about this violation becomes part of the black list.

One may not like this, but in this case one will not like the network. So the first users of the network will be those who accept this principle, who accept that freedom means also acceptance of the consequences of the own bad decisions, who reject paternalism by government. There will be not much sympathy for those losers who cry for government for help.

Mutual support in case of failure is another question: There will be insurance companies as well as organizations for mutual help in case of necessity. But it should be noted that there is a danger: The first users may be those who don't care much about this, accepting the ideology that one has to pay for the own errors. Thus, the problem of creating an appropriate infrastructure for helping the poor may be

ignored. This can give a base for a revival of ideologies in favour of paternalism by some central government.

This is, essentially, what has happened after the crash of communism in the West: Instead of transforming the social security system into something compatible with free markets, it has been heavily reduced. As a consequence, it has become possible for marxistic ideology to revive.

4.4. **High value of truth.** With the network, it becomes much harder to cheat and to lie: One can ask the suspected liar to put his lies in form of a promise into the network. His refusal to do so strongly suggests that one should not believe him. Instead, if he accepts this, he risks a lot, in particular a record in the black list. This makes the network much more attractive for those who have a high value for truth.

Now, it may be argued that this does not make a difference: Truth is a high value even today. But this is not really the case. Politicians in a democracy and journalists in democratic mass media are notorious liars, not because they are inherently bad, but because one cannot survive in these businesses without telling lies. Most intelligent people have more or less accepted, as a fact of life, that one cannot believe politicians and mass media (possibly with some exceptions for a few high quality journals).

The ideal of truth-seeking is much stronger and more common among scientists. A probable consequence is that scientists themself as well as scientific values will become more popular in the network.

4.5. **Political anarchism and the Golden Rule.** There is one reasonable and plausible meta-rule: The Golden Rule. It is likely to be accepted by many participants.

Indeed, once the participants will have rules which differ, and, in particular, differ from the laws of the particular governments, there is a strong incentive to justify this difference in a moral way, by moral argumentation. Now, the Golden Rule gives such a justification in a quite general form: It forbids (in a quite natural interpretation) any legal monopoly of some person or organization, thus, in essence, forbids states, which depend on such legal monopolies, in particular on the monopoly of the use of force.

Therefore it seems quite likely that political anarchism – the ideology which rejects the state as amoral, in particular as violating the Golden Rule – will be quite popular in the network. In particular, it will be extremely popular among those who use the network for illegal activities: The obvious reason is that they have not only an ideological, but also a real conflict with the laws of the government. This will be used by opponents to suggest that political anarchists and network users in general have criminal interests. But who cares? Given the density of government regulations in almost every domain of live and the stupidity of many of these regulations, most people have at least some illegal interests, even if it is only copyright violation or tax avoidance. Given the possibilities of the network to realize them, one can expect that they will be used. An ideology which justifies this behaviour will become popular among the network users.

5. Free discussions and its consequences

The network also gives unrestricted, uncensorable free speech. This includes all types of free speech, including pornographic speech, hate speech, and distribution of dangerous information. Those who favour the network consider this as an important advantage: Whatever their personal reasons (may be they simply like forbidden porn), they can use general political arguments to justify this. Thus, there will be also a strong support for unrestricted freedom of speech.

But freedom of speech has some other, implicit consequences for the ideologies which will become more popular.

5.1. **Freedom of speech in a democracy.** Freedom of speech is a value in democracy, but it in no way means that all political opinions have a chance in the mass media. The mass media present only a surprisingly small part of the different political theories and ideologies.

The reason for this is the way democracy works, especially in the case when there are only two big parties. Only one of them will win, but to win the election, the best position is the center. As a consequence, above big parties will fight for the center, and, therefore, present to the public almost identical political positions. Their political fight is, of course, a real fight, but only for power: Their political position is almost the same, the differences are only minimal. Even if some of the politicians in these parties have other opinions for themself, they will be unable to express them openly if they are in conflict with the position of the center.

The democratic mass media hide this. The media like to present the minimal differences in the political positions as important, big differences, even if they are only minimal disagreements about almost unimportant particularities. Presented in such a way, the agreement about all the questions shared by the two big parties looks like agreement of a great majority – of all those who vote for the two big parties. It isn't. People have, at best, not thought about those questions which are consensus among the great parties. If they have, they often disagree, but nonetheless vote for one of the big parties, the one less evil, because everything else would mean a loss of their vote.

But the alternatives, outside the mainstream, are seldom discussed. If politicians of the great parties participate, they reject them in full agreement as nonsensical, radical or worse, and after this discuss their minor disagreements about how to fight them. What they share is the agreement that "one should not give a forum to these positions". This is far away from the ideal of democratic discussion, but it is how democratic mass media work.

5.2. **Freedom of speech in the network.** What changes with the network? Every position can be presented, in as much detail as one likes, in the network. In part, this already happens in the usual web, but only in part: Some of the positions already cannot be presented today openly in the internet, the world-wide censorship has heavily increased during the last years. The network cannot be censored as easy as the internet, because all what is presented pseudonymously cannot be traced back to real persons. There is also no provider of a particular site who can be forced to shut down the site. Censorship simply will be technically impossible without suppressing the network as a whole.

When, there will be uncensored discussion forums as well. Now, uncensored discussion forums have some problems. The main problem is that there are lot's

of crank participants with extremely dubious positions which most of the readers would like to ignore. The classical way to handle this problem is the so-called killfile: A list of people one does not want to read. Unfortunately, the cranks don't like them and often change their names. Then, spamming is another problem. As well, discussions in the net show a tendency to become more heated and aggressive than real live discussions. But these problems are solvable. In the worst case, moderated discussion groups are a solution.

So, every political and ideological position can represent itself in the network. As well, in appropriately organized discussion forums every ideological position can be discussed and criticized from all other political positions.

5.3. **Increase of internal consistency.** Unfortunately, it is not that easy that the best position easily wins in such discussions.

One reason is that different political and ideological positions are often based on different positions about the facts of real life. But it is hard to evaluate claims about what happens in real life reading only a discussion about it.

The easiest thing which can be evaluated is the internal consistency of some position. As a consequence, one has to expect, as a first consequence of free speech, that the winning positions are more internally consistent. The participants of such discussions do not have to win elections, they have to win discussions. You win discussions if your opponents have no good arguments against you, but any internal contradiction in your position is a good argument – very powerful because everybody can see such internal contradictions, without having to check the facts, and (for the same reason) it is much easier for your opponents to find such arguments.

This heavily distinguishes them from the mainstream position defended by democratic parties. The position defended by mass media and politicians can be described in a very simple way: Take a questionaire with all the politically relevant questions and ask some institute to find out the majority opinion about each of them. The resulting position is the position which is likely to give you the support of the majority in elections. This is obviously not a way to obtain a consistent position. But in TV discussions this does not matter much – the attention span is much to small, and those who are nonetheless able to catch the contradictions cannot simply start to participate, as they can in a discussion forum.

Therefore one could expect that internally consistent positions become more popular in the network, while the democratic majority opinion – a contradictory mix of popular prejudices which wins in democratic parties and elections – will loose support.

5.4. **Radicalization of the content of ideologies.** There is only one correct consistent position. Unfortunately, there are much more wrong but consistent positions. And one characteristic property of wrong consistent positions is that they may be heavily wrong – sometimes much more wrong than the contradictory compromise position defended by democratic parties. And they radically differ from other internally consistent positions, much more than the positions of the great political parties which defend essentially the same mainstream position.

Of course, we may hope that, in the long run, the truth will win. But in a short run we have to expect a radicalization of society. The democratic consent position will be the loser: It is full of inconsistencies, of political compromise, of nonsense

which cannot be defended in a consistent way in uncensored discussion. Instead, radical positions are often much more internally consistent.

In particular, the moderate, civilized Western versions of Christian religion are quite inconsistent with the Bible text. Christian fundamentalism is much more internally consistent. The moderate Christian is usually shocked if confronted with the parts of the Bible where God requires murder of innocents and genocide. For the fundamentalist, this is not an argument at all. If God tell's us to kill, let's kill. Such radical positions can win arguments because of their consistency. This is not accidental: It is the search for consistency which has caused the development of many radical proposals. Thus, one has to expect some rise of fundamentalism, in comparison with more civilized, less dangerous versions of Christianity. The same has to be expected for all the other religions too.

But as well there will be a rise of consequent atheism too: First, as a reaction to the increasing danger to humanity from the more and more fundamentalist religions, but also for the same reason of internal consistency – the rejection of religions is much more consistent than the sort of moderate acceptance of peaceful religious beliefs and the refusal to fight them as wrong and misguided which is typical for democratic parties.

This is quite close to what we observe: Radical islam, as well as radical christianity, have become much more powerful and influential in the last twenty years, and, as far as I know, other religions also show such tendencies. But atheism is also increasing: the movement of the brights is evidence for this. Another evidence is that libertarianism is becoming more influental too. Instead, the established, moderate versions of the various religions seem to lose.

In fact, this argument is not a prediction, but an explanation – the result of the author's attempts to understand the reasons for the rise of fundamentalism in the age of the internet. This explanation also fits nicely with the fact that islamist extremists use the internet as well as that they are often from middle-class or even rich origin.

5.5. **Why it makes no sense to kill the ideological enemies.** But considering the dangers of radicalization, we should not forget another effect which diminishes the most dangerous form of radicalism: In the network there is simply no possibility to silent the opposition to the own ideas by killing or incarcerating them all. This measure is simply not effective: If it becomes only slightly uncomfortable to defend some point of view in the open, one can always use a pseudonym to defend it. Thus, long before somebody proposes to kill or incarcerate all the opponents, at least some of these opponents, enough to defend the position, will have switched to pseudonyms. This does not decrease their argumentative influence – everybody can read them – but prevents all the repressive measures.

Therefore, while more radical from point of view of the content of the proposed ideologies, at least some proponents of these ideologies will have to continue to discuss their ideology with the opponents: Else, the opponents simply have the last word in the open discussion forums which will be accessible to everybody.

Thus, the picture may be quite different from the scheme of ideological opposition in the past: While the factual differences between Stalinists and Trotzkyists, shiits and sunnits, catholics and protestants have been minor in comparison with the part they have shared, they have killed each other merciless. In the network, proponents of quite opposite ideologies, who share almost nothing, may peacefully (even if

hatefully) discuss with each other. This happens not because they have become full of love for their enemies, or understood the value of free speech for society, but simply because they have no chance to kill their opponents, and because finishing the discussion means to loose the ideological battle.

5.6. **The other side: Increasing complexity.** Political discussions in mass media, in particular TV, have only an extremely short attention span: One cannot present an argument which needs more than half a minute for explanation.

This is different in discussion forums and on websites: Here, arguments can be worked out in much more detail. Moreover, all sorts of books will be available for free (no costs for copying and no copyright restrictions), making them much more accessible.

Thus, the complexity of the ideologies and in particular of the arguments about them is much less restricted than in democracy.

This effect is clearly positive: To see the contradictions in the standard democratic ideology, but also the problems of the various extremist solutions (which are usually based on radical simplifications), one needs more than the half a minute mass media attention span. The chances of simple populist ideologies decrease.

5.7. **Rationality of the resulting ideology.** It has often been noted that democracy requires some irrationality of the majority. In particular, the participation in the election is highly irrational: The probability that the own vote decides the election is close to zero. In comparison with this, it is irrational to go to the election, and even more irrational to spend time for decision-making about this choice.

A remnant of this irrationality is that the choice made is highly irrational, and much more stupid than the choice of the average citizen if one would give him the opportunity to decide about this question after learning about the relevant facts some time. In this case, this same person would spend more time and be more interested to find out the best solution. Instead, arguments during election campains have to take into account that the attention span is not more than half a minute. To explain something more complicate is a waste of TV time, because nobody would care, given that it is irrational to care at all about elections.

This central irrationality of democratic elections does not exist in the network. Here, if you care about your rules, you will gain the advantages, if not, you will have to pay for your accepting bad rules. Thus, it is rational to care about them. It is also rational to behave honourably, much more rational than in a democracy, where you can behave unhonourably as long as this does not violate the laws, or the fines are too small to deter you.

5.8. **Summary.** We have been able to identify some ideological tendencies which with high probability will be related with the network.

The revival of values related with honour, as well as the increasing role of self-determination, seem quite natural. Look at the games of children: Even today, their heros behave honourably and show a lot of self-determination, without caring too much about democratic values. They also love freedom of speech: They like to use forbidden words even if they don't know their meaning. So the new ideological values themself are easy to understand even by analphabets. In their environments, honour plays a more important role even today, and they often self-determine themself in conflict with established society.

Honour and self-determination as ideological values are also a good starting point for a new generation to fight their parents: To distinguish themself from the older generation via music, clothings, or drug use has exhausted itself.

A certain radicalization of society, based on the rejection, at first, of the inconsistent democratic consensus ideology, is what we already observe. This is what would be favoured by a new generation of protesters as well as truth seakers: Before finding truth, one has to go through some errors, and these errors will be often consistent but radical theories.

Fortunately, this radicalization, if it happens in a situation of real free speech, is not that dangerous – it is only the intermediate result of the search for truth: Radical ideologies are attractive, because they combine consistency with simplicity. But they have their weak points, and to fight them is not hopeless at all.

The point of free speech supported technically, within a network which allows pseudonyms, is that it prevents the main reason for radical ideologies becoming dangerous for their environments: The wish to kill or otherwise silent their opposition. Most mass murder has not occurred between ideologies which have been radically different, but between ideologies sufficiently close to each other – religions or ideologies which have shared the same Holy Scripts like the Old Testament, or Marx's "Das Kapital". Thus, it is not the large difference between ideologies which causes mass murder: Instead, mass murder is a way to solve the problem with the opposition if you lose in a free discussion. But in the network, this is no longer a way to solve the problem. Therefore widely different, radical ideologies in themself are much less problematic as it seems at a first look.

6. The problems of small minorities

One cannot be forced to accept rules? That's quite naive. Of course one can. The moral pressure of society can be very strong. In fact, only a few very strong people are strong enough to resist if all around them have the same opinion about some question, even if the complete stupidity of the majority opinion seems obvious to any non-prejudiced outsider.

6.1. **Difference to democracy.** Nonetheless, the majority has a much harder job to enforce something on minorities than in a democracy. Last but not least, in a democracy 51% seem sufficient to apply a law, which prescribes to everybody what the majority likes, and penalizes everybody who does not follow this law. But 51% of having another opinion is nothing one would even have to care about in the network society. Even 95% are not that problematic, at least if the 5% are concentrated in some regions.

And even if the majority is overwhelming, there will be some outsiders who do not accept the moral rule of the majority. At least these outsiders have some advantage from not accepting the majority opinion – even if they have to pay for it with some forms of boycott. Moreover, these outsiders can easily find similar minded people – other outsiders in the same or different questions, as well as those which are more tolerant – and organize small support networks or local communities.

6.2. **The impossibility to prevent the establishment of real life networks.** Then, the owners of the pseudonyms can meet each other in real life too. Every human needs support form others, support from people with similar ideas, and this need of support is powerful enough to make people taking large risks. Even during

Stalin's terror there have been people close enough to each other, with enough trust into each other, to talk about forbidden things and to make jokes about Stalin. These private networks have been extremely small and rare, Stalin's regime has tried it's best to reduce them, but has nonetheless been unable to destroy them completely. Thus, it seems very unlikely that people who can meet in the network pseudonymously, talk and joke about everything, would not meet each other in real life too. Last but not least, a lot of communication is one of the best ways to establish trust into each other, and communication itself would not be risky at all.

Note that the role of the network in such a situation is completely different: The pseudonyms do not rely on the power related with the black list. If an pseudonym appears on the black list, nothing happens to the real person, which remains unknown: It is a free decision if a pseudonym establishes a connections with some non-pseudonymous account, and in this situation where is no good reason to do this. All what they use is the power of communication.

Last but not least, let's mention in this context the points we have discussed elsewhere: The high ideological value of self-determination in the network, and the consequences of free pseudonymous speech – in particular, the meaninglessness to kill ideological enemies. Above points restrict, in particular, the power and will of the majority to suppress minorities.

6.3. **Self-defense of the majority remains possible.** Thus, the majority has a much harder job than in democracy to repress minority opinions. But this is not only a positive effect: Repressed minorities are not automatically unjustly repressed. There are minorities, like terrorists, which are really dangerous for their environment. What about them?

Now, the right of the majority to self-defense is not questioned at all by the network. One can accept rules which allows a sufficient amount of self-defense against such dangerous minorities.

But what is the boundary between reasonable self-defense and aggression against a minority which only claims to be self-defense? This question is clearly not answered by the network, and it cannot be answered with such purely formal and technical means.

The boundary between aggression and self-defense will always remain problematic

But this does not mean that nothing changes: It depends on the environment which measures of prevention have a chance. Given the network, it becomes a purely technical impossibility to prevent some forms of communication between the "enemies". So, it will become unlikely that the majority attacks in unjustified "self-defense" these communications.

7. Standards for law codes

A world with more than 6 000 000 000 different law codes seems to be completely unmanagable. But is it? We have a revolution in information technology, and this revolution allows you already today to put a name into a search engine like Google and to find out almost everything written about the person in question. The search itself requires almost no time at all, much less than you need to find a paragraph with known number in a penal code in non-electronic form. So maybe this revolution in information technology gives us the ability to handle 6 000 000 000 different law codes too?

7.1. **The basic idea of a standard for a law code.** In fact, it is possible. All what is necessary is some form of standardization of the law code – it is no longer an arbitrary simple text.

This seems restrictive. But it is much less restrictive as one thinks if one hears "standard". In fact, imagine you have the right to change all the numbers, but only the numbers, in the penal code of your country. In particular it is allowed to change all penalties, and to set them to 0 for everything you want to legalize. Wouldn't this be sufficient for you?

But this is all standardization we need. Numbers are a simple thing, simple programs can be used to compare them. The meaning of each number is fixed by the standard, but the number itself can be changed. So, the basic idea of a standard is simple: It is a complete law code, as the law codes we use today, except that all the numbers in the code, especially all the penalties, are not fixed, but can be freely, and differently, chosen by everybody who uses this standard.

Given such a standard, we are almost free to design a fair, just law code by fixing appropriate numbers for the penalties. So, the law code we use consists of two parts: The reference to the text of the standard, and a large table which contains all the numbers we can specify.

With such a standard we can easily evaluate the law codes of other people: This can be done by a simple program. All the program needs is another table of numbers, close to the one you have used for your just law code, but possibly different, together with a table of error margins which defines your personal degree of tolerance. Then, the program simply has to check if the numbers of a given law code are inside the margins you have specified. These data you have to define only once. After this, you can use the same program to evaluate everybody else. You can even use the program in your search engines to evaluate large numbers of people. This is possible, because the job of the program is extremely simple and fast – it has to do only elementary comparisons.

But even if this is too much work for you – to fix all these numbers yourself – you can start by copying the numbers from somebody else, from somebody you trust. Then you have already a set of numbers for your own laws as well as for your evaluation program. Then, if you find some time or have some other reason to change something, you can change a few numbers of your choice.

7.2. **The advantages of standardization.** But how one can establish a good standard? Maybe in a world where everyone separates no such standard will appear? There is no such standard even today, among a few hundred states. How can one imagine that such a standard may be established between billions of people?

The reason is simple: Different states do not have to cooperate very much. They have their own territories and borders. It is nice if the border is a peaceful one, and if it is allowed to cross it. But it is not a necessity for states. The situation is very different for people. They have to cooperate. And, in a situation where everybody has different rules, a presupposition for cooperation is that the rules are sufficiently compatible. So, for people there is a necessity to make their rules compatible. So there should be, as a minimum, a way to establish if they are compatible or not.

The proposal to follow some standard is, therefore, a reasonable one. If there is a group of people who prefers some standard, it is a good idea to join them: It makes your rules comparable with their rules. So you can find out the subset of people of this group with rules compatible with your own wishes. And they, in turn, can

compare your rules with their own wishes. If this gives sufficient agreement, you can start to find a compromise about the remaining open questions and, then, you can start to cooperate.

And, if they use a standard which follows the scheme described above, the comparison itself will be extremely fast.

The advantage to use such a standard obviously increases with the number of people who use this standard. You have simply more people who can be checked, and therefore the probability that you find somebody to cooperate increases.

But this property alone – the utility increases if more people are using a given tool – is sufficient for a natural monopoly. So, a standard will appear. And it will appear in a very short time, for the simple reason that without a standard the whole network makes not much sense: You have no way to find people with compatible rules. But cooperation is a necessity. On the other hands, it is risky to cooperate with somebody who does not accept reasonable rules of behaviour. So to have some way to compare the rules is extremely useful to you. And because it is extremely useful for those you want to cooperate with, it is reasonable for you to provide the information they need.

One should not forget that there is competion for cooperation. Other people who may like to cooperate with me, can as well make another choice and cooperate in the same question with somebody else instead. Once they use an evaluation program which relies on some standard to make this choice, it would be stupid for me not to provide the numbers this program needs.

7.3. **Competition between different standards.** So it is useful for everybody to accept an established standard. But maybe the established standard is stupid? Is it possible to shift from one standard to a better one? It is, and the aim of this section is to explain how this can be reached.

The idea is quite simple – those who propose a new standard simply have to provide automatic tools for the transformation of the numbers of the two standards. Then, a program which uses one standard for comparison can be easily modified to be able to use the new standard as well – all it has to do is to transform the numbers using this transformation procedure if somebody uses the new standard.

The transformation programs allow also another way to switch. I want to switch to the new, better standard. So, I start with the transformation program, in one direction, to obtain a starting point for the new standard. Then I modify the new numbers using the new possibilities of the new standard. From now on I care only about them. So, to switch is quite easy. On the other hand, I can continue to support those who use the old evaluation programs and give them the numbers for the old standard. Here I have even two possibilities: The first one is to leave the old numbers as they are. The second one is to transform the actual numbers of the new standard using the transformation program in the other direction.

What makes the transformation to a new standard unproblematic is that one is not fixed to a single standard. If one has appropriate automatical transformation functions, one can support all standards by using a single preferred one and then supporting all others by automatical transformation.

7.4. **Transformation programs between standards.** Let's consider now the problems related with such transformations in more detail. We have to solve the following problem: We have two different law codes, say those of different states.

One of them is filled with numbers, the other not. Is it difficult to find numbers for the second code so that the result is at least close to the original? What are the rules for such a transformation? There are different situations which have to be considered here:

7.4.1. *Splitting an article into several.* A quite typical difference between different law codes is that one article of one law code is splitted into several articles of the other code.

In one direction, there is no problem at all: We have penalties for the single article of the first code. Then we can simply use these for all the corresponding articles of the other code.

In the other direction, this seems more problematic: We have different penalties for the different articles and have to combine them now. But if the penalties are given as a range between a minimum penalty and a maximum penalty, we have a natural rule for unification:

- The unified minimum penalty is the minimum of all the minimum penalties;
- The unified maximum penalty is the maximum of all the maximum penalties;

7.4.2. *Introducing a new article.* Another typical difference between law codes is that one contains an article which simply does not exist in the other.

But to define transformation rules is trivial in this case. The non-existing article is equivalent to the same article with minimum as well as maximum penalty of 0.

7.4.3. *Splitting a fixed penalty into a range.* It is quite usual to define penalties using a range between a minimum penalty and a maximum penalty. But it is also possible to have only a single, fixed penalty. The problem with this is that different violations have to penalized in the same way. But, on the other hand, it minimizes complaints about the particular arbiter being too strong or too mild. So there are advantages as well as problems, and one cannot completely reject one method.

Now, in the first direction, there is no problem: The fixed penalty becomes the new minimum as well as the new maximum penalty.

In the other direction, the decision seems more arbitrary, but there are three natural choices:

- the harsh one: The old maximum becomes the new fixed penalty.
- the mild one: The old minimum becomes the new fixed penalty.
- the average: The arithmetic average between the old minimum and the old maximum becomes the new fixed penalty.

But there is no problem in principle with a transformation program which depends on some parameters. Those who apply the transformation program are then free to choose particular values.

7.4.4. *Introducing degrees of seriousness.* There is a quite typical difference which is, in fact, a particular example of splitting a single article into several but which requires a more detailes consideration: The introduction of degrees of seriousness. The problem is that the transformation rules we have defined above – to use the same penalties for all new articles – seems unnatural in this case. It would seem more natural to increase the minimum penalty for the more serious degree and to decrease the maximum penalty for the less serious degree.

But how much? Here, again, one can introduce some parameters. Who wants to use the transformation program is, then, free to modify these paramaters.

7.4.5. *Shifts of the meaning.* A much more difficult thing which is also quite common is a shift in the meaning of the words.

But at least in principle one can subdivide this problem into a combination of the already considered cases. If there is a shift in the meaning, there will be some sort of behaviour not covered by the one article but covered by the other one. But in this case, we can identify this with a case of splitting. The article which covers the behaviour in question is splitted into two – the article which does not cover it, and a new article which covers only the behaviour not covered by the old one. So we can apply the rules of splitting with the rules for introducing a new paragraph.

There are situations where the result may look not optimal. Imagine a crime with some nontrivial minimum penalty is slightly extended and covers now previously legal behaviour. Applying the rules as described above would reduce the minimum penalty to 0. Here, again, one may want to introduce some parameters which modify the rules for splitting: If the splitting consists of one much more important part and some exceptional cases, the new minimum may be something higher than the minimum of the minimal penalties, closer to the minimum of the main penalty.

7.4.6. *Summary.* So it seems quite reasonable to expect that a modification of the standard can be supported by reasonable and adequate transformation programs.

To define appropriate transformation rules cannot be automatized completely – to establish that the meaning of one article of one code is equivalent or at least very similar to another article of another code is something which requires understanding of the meaning of above articles. Without artificial intelligence, this has to be done by humans.

But it has to be done only once for each new standard. The rules we have found do not depend on the particular numbers for the penalties, thus, are the same whatever the particular penalties proposed by the users. So everybody can use the same transformation program. This transformation program has to be written only once.

It will be provided by those who want to establish the new standard. These people already knew the old as well as the new standard – the old one because their decision to develop a new one was caused by some discomfort with the old standard, and the new one because they have designed it. So it will not be problematic for them to write an appropriate transfer program.

Given that proposals of a new standard come in combination with transfer programs between the new standard and the old, established ones, to switch to a new standard is easy for everybody – for those who decide about their own laws as well as for those who want to use programs to evaluate the law codes of others.

So it is unlikely that a bad standard will win. The problem of all hardware standards, but also of many software standards, that to switch to a better standard leads to high costs, is not present in this case. Everything what is necessary for a simple switch to a better standard can be easily provided by those who propose the new standard.

Moreover, if transformation programs are available, people who prefer a minority standard are not forced to follow the majority standard. They can, instead, use their own preferred standard and then use the transformation program to create the

data for the majority standard. This property also descreases the risk of switching to a new standard: If necessary, I can continue to use the new standard even if it fails to be accepted by a majority. This is important because it increases the probability that a really better proposal for a new standard becomes accepted.

Therefore one can expect that the standard which becomes established by free competition between providers of standards will be a quite optimal one.

7.5. **What will be the differences between the competing standards?** There are a lot of things to be optimized in law codes even if the penalties remain unspecified.

The following things are quite obviously useful criteria for optimization:

- Comparability: An article should cover only a certain type of dangerous or harmful behaviour which is specific enough so that any behaviour covered by the article is of comparable seriousness (that means, causes comparable harm or can cause such harm with comparable probability, and is associated with a comparable degree of guilt). If the same article covers extremely different behaviour, which shares only a few details which are quite irrelevant in comparison with the differences (as, for example, rape and volitional sex share sex) the article will lead to injustice: The same minimum and maximum penalties will be applied to quite different behaviour. So or the minimum penalty is far too harsh, or the maximum penalty is far too mild, or the range between them is too large so that too much is left to the personal preferences of the arbiter.

  Often political fight in democracies leads to compromises where an article is extended so that it covers, in the extended form, quite different things. There is no reason to do such things in the development of standards.
- Certainty: It should be easy to decide if a behaviour fits into the article or not. Vague articles are horrible – they leave far too much to the freedom of choice of the arbiter. Vague articles have advantages for those who apply them like judges in states. But they are dangerous for the people, because one may be misguided by an interpretation of the vague notions and end in prison if the judge prefers another one.

  Vague notions often appear in state laws as a compromise between different political directions. There is no reason for such vagueness for the developers of standards.
- Good design of an article will show up in the penalties people assign. Uncertain articles will tend to give a much larger range of penalties than certain articles. In articles which cover only comparable behaviour, the range between minimum and maximum penalty will be in the average much smaller. Thus, one can even use statistics to evaluate the design of particular articles.

There are other aspects of a good law code. In fact, the behaviour described in different articles have a lot in common. So in a just law code there would be certain relations between the penalties for different articles, with comparable penalties for behaviour of comparable seriousness. How to organize law codes in such a way that this is easily maintained is a complicate question. One way to solve this is to distinguish, in a general part, various qualifying circumstances (intentional or not,

how many instances and so on) and how they modify the penalty, which is defined in another part.

Then, usually there are, in support of the penal code, commentaries. Today these commentaries often refer to particular cases, with decisions of higher courts about them, and they interpret the meaning of the words of the articles. These interpretations are not optimal, in the sense that they are not optimized in the light of our criteria of certainty and of coverage of cases of comparable seriousness. Instead, they are the results of political and legal fights: Political fights, which often lead to a vague compromise, and subsequent legal fights about their interpretation. In the standards which will develop in the network, these commentaries will be part of the code, and designed by the originator of the code to be optimal in the light of the criteria.

It is important to note that the development of the code will not be distorted by political questions which often distort law-making. The point is that even if the code designer has some political intentions, these are usually irrelevant because the penalties cannot be specified by the code designer. Instead, if a politician wants to enforce a high penalty for behaviour A, it may be useful for him to combine it with a dangerous crime B into a single article. Then he can insist in his popular speeches on a serious penalty for crime B to obtain in this way a high penalty for crime A. In the network, this will not work. Combining A and B may, instead, lead to a far too low penalty for B. Indeed, to establish a penalty for the article many people will care, in favour of the potentially accused (that means, for themself), about the least serious variant, which is, in this case, A. So, those who follow this principle will establish the lower penalty for the combined article. Other people will disagree, and establish the higher penalty. But such a large difference in the penalties considered as just by different people will result in bad statistical results for the combined article.

Even more, everybody who thinks that A and B deserve different penalties will not like the whole code. In the other direction, there is no such problem: Those who think that A and B are comparable will not reject a code which distinguishes them – they will simply assign the same penalties to above articles.

Thus, what is a reasonable and rational strategy in the political fight becomes stupid for the code designer in the network, and will lead to a rejection of his proposal.

So one can expect that the standards developed in a free competition will have a much higher quality than the actual laws of states. The articles will be more certain, easier to interpret, and cover behaviour of comparable seriousness.

7.6. **Translations of the law codes.** There is also another aspect of the standards developed in the network: The aim of the designer is to win the competition in the whole world. So he has, of course, to translate the code as accurate as possible into all languages of the world. A code which is badly translated leads to conflicts between people using different languages. And if a code is not translated at all into my preferred language, I will not use that code. If it is badly translated, and I hear about this, I will switch to a code which is known to be better translated. So, the winning standard will be not only translated into almost all languages, but translated in high quality.

An important point is here that the commentaries are part of the code. The words of the articles may have different meanings in different languages, but the

commentaries (which will be, of course, translated too) may be used to correct possible misunderstandings.

7.7. **Summary.** Thus, from a pure technical point of view a world where everybody accepts a different set of laws and rules is managable. Managable already with the technical possibilities available today. There is no need to hope for further improvement of our computers.

We can expect that free competition will in a short time lead to some standardization of the law code in such a form that the text of the articles is fixed but the penalties themself will be left to the free choice of the participants. There will be further competition for the best proposal for such a standard, and one can reasonably expect that this leads to an important improvement of this standard in comparison with actual law codes of actual states. In particular, the standard will be supported by accurate translations into all important if not all languages.

The amount of information to be stored for all laws of all people in such a standard is sufficiently small. Let's estimate it: A standard penal code has a few hundreds of articles. The penalties are usually defined in a quite coarse way, so a single byte, which allows 256 different choices for the penalty, would be sufficient. So, one would need a few hundred bytes for every person. With $6 \cdot 10^9$ people on Earth, a few hundred Gigabyte will be sufficient to store the law codes of all people on Earth. Or, in other words, the storage of your laptop may be already sufficient.

8. Forgiving black list records

What to do with people on the black list? If there would be only the information "X has broken a promise" it would be quite hard to decide if one can trust him in any future.

But there are some simple and reasonable ways to support you with additional information about the particular event, information which you can use to make a reasonable decision about forgiving.

One idea should be excluded from the start: To delete entries from the black list after some time. This would be simply nonsensical and unenforceable. Information which has been given once can be stored. There have to be several copies of the black list anyway, for the very security of the network itself, and there simply will be no central instance to delete. And it would be in contradiction with the very idea of the network that everybody is free to decide himself about forgiving.

Forgiving is reasonable and rational. It does not make much sense to reject everybody who has broken an own promise once and forever. There are, instead, many circumstances which may motivate a decision to forgive. And one can support this process of forgiving by supporting adequate information which allows to decide about this even automatically. Let's consider some examples here:

8.1. **Children in the network.** There is no age control in the network. It is open to children as well as adults. Nobody can be excluded. To exclude children would violate not only the very idea of the network, it would be also problematic for other reasons: One would like to have a possibility for pseudonymous accounts too. This is important for the survival of the network if it is forbidden by the state. A pseudonymous account also needs full control of all the information he decides to publish in the network. This includes, of course, his age. So, nobody is obliged to give information about his age.

Given this basic principle, it is simply impossible to exclude children. And, once it is impossible anyway, it makes no sense to exclude them if they decide to tell us their age.

Now, in the laws of the state, children cannot be punished below a certain age. Here, the network will behave differently. Whatever happens, the arbiters only establish facts and follow their rules. So, if a child breaks his promises, and somebody else objects, there will be no exception – the record about the broken promise will be published in the black list.

And, in fact, it makes no sense to make exceptions for children. One could, for example, imagine an arbiter who openly claimes that he will not decide against children below a certain age. But that means, one cannot trust this arbiter to judge in general about pseudonyms. Last but not least, one cannot be sure that there is no child hidden behind the pseudonym. And it would not help a child which openly acknowledges his age to accept this arbiter – it would have to find other arbiters anyway. So, the decision of the arbiter harms himself and does not help the child.

On the other hand, it is not that problematic for a child to appear on the black list as it is for an adult. In fact, most people believe that the errors of children should be forgiven very fast. But there is a simple way to do this automatically: The child simply informs everybody about his date of birth.[1] But if we know the date of birth, and we also know the date when the promise was broken, we know the age when the child has broken his promise. And we can decide about our personal preferences for the relevant ages limits.

These age limits can be given to the program which we use to evaluate the black list. And the program can, then, automatically ignore all records caused by children below your age limit. So, the question what is the appropriate age limit will be decided by everybody himself.

If a child uses a pseudonymous account and does not give the information about its birthday, one cannot use this way to forgive. But this is the free decision of the child itself.

It should be noted that children have an interest not to tell about their birthday. There are, last but not least, a lot of adults who think that one cannot cooperate with children because one cannot trust them. These will be probably the same people who will easily forgive children.

8.2. **Newbie errors.** Similar to the errors of children it seems reasonable to forgive errors made by newbies. To support this type of decision, the record will contain also the date of becoming a member of the network. So, completely similar to the birthday of a child, the "birthday of membership" may be used to classify a record which appears almost immediately after as a newbie error and to forgive it.

Here one has to care, of course, about the possibility of an earlier pseudonymous membership. Indeed, if somebody has a long experience in the network using various pure pseudonymous accounts, it is not very reasonable to forgive him a newbie error after he starts to use a personal account with his real data. But there is nothing one can do against this possibility, except for not allowing pseudonymous accounts at all. But this would be problematic and not useful at all.

So I would guess that forgiving newbie errors will not be very popular. But, whatever, everybody is free to decide about this himself.

[1]How such information can be made trustworthy is another question which will be considered later.

8.3. **Penalties as information about the seriousness of the broken promise.** To appear on the black list is not something one would like to experience. One way to avoid this is to accept penalties different from a record on the black list. So, by breaking the rule one risks only the penalty.

But the black list nonetheless does not disappear completely: In fact, to accept the penalty is also a promise in itself. That means, for evasion of paying the fine, or for running away from the jail or the working hours or other ways to avoid the penalty given in the first round, there will be a second decision. And now the penalty has a form that one cannot run away from it – the record in the black list.

Nonetheless, the idea to replace the black list, as a penalty, by other penalties seems a reasonable one. It is safer for you. Moreover, the potential cooperators will not punish you for this idea – instead, they will even favour a fine to be paid them in comparison with an entry in the black list which they cannot use to buy something.

So we can expect that the idea to use penalties different from black list entries becomes a standard. In fact, in our consideration about the standardization in section 7 we have implicitly already assumed this. This gives a new possibility to evaluate, in a quite automatical way, the seriousness of a broken promise. Indeed, a record in the black list will be not about some completely general promise, but for the avoidance of the penalty established in the first round. But a penalty has a number, and this number will be part of the record.

So, all one needs is a way to extract the size of the penalty from the record about the broken promise. This can be supported by a standard place where this number will be written down, so that the program does not have to be clever to find it.

This size can now be used as a characterization of the seriousness of the broken promise. This is an important and useful information if one wants to establish what to forgive after which period of time.

8.3.1. *The evaluation of promise without penalty.* In principle, nobody forbids to use a record in the black list immediately as a penalty, without any other penalty. In this case, the question is how to estimate the seriousness of the broken promise. One could think that, once no information is given, the broken promise was a very serious one. If many people would follow this idea, this would be problematic for those who have broken only a harmless promise and used no other penalty than the black list.

But it would be easy to avoid this, by assigning additionally a symbolic penalty of, say, 1 cent. Then this additional penalty would appear as the penalty which is relevant for establishing the seriousness of the broken promise. In the light of this possibility, it seems much more reasonable to interpret the broken promise without any penalty except the record in the black list as a really harmless one. Indeed, it would be strange to decrease the degree of seriousness if the penalty is increased from 0 cent to 1 cent.

Therefore, the natural and reasonable choice to establish the seriousness of a promise without a penalty other than the black list record is to classify it as the most harmless one. But it does not follow at all that such an entry is harmless too. Even a harmless broken promise is a broken promise, and there may be many people who don't forgive, or, at least, don't forgive completely.

8.4. **Limitation.** A more important criterion for forgiving would be a sufficently long time between the date of the broken promise and the actual date. As already mentioned, the date of the broken promise, if known, will be part of the record. If it is not known, there will be anyway the date of the decision about this case. This date is obviously known by the arbiter and is an obligatory part of the record.

And, certainly, knowing that many people will forgive after a few years, but would be unable to forgive if no date is known, it is in the very interest of the rule-breaker that not only the date of the decision, but the earlier date of the broken promise will be part of the record.

So, everybody can decide himself about his personal statute of limitations. He can (and will) use for this purpose the information about the seriousness of the broken promise, as defined by the penalty. And, of course, he can use other limitations in dependence of other circumstances, like the age.

8.5. **Explicit forgiving by the victim.** There is one possibility which seems useful to add: The victim of the broken promise may be allowed to add an explicit decision to forgive. One can imagine that it has some personal reasons to forgive. Quite probable, the promise breaker has done something to deserve forgiving, for example paid the fine later.

One may be, of course, afraid that the victim may have been blackmailed to forgive. But this does not seem quite probable. Indeed, if there would have been a way to blackmail the victim, one would expect that it would have been used earlier, and the record would not have appeared at all. So it seems reasonable to follow the victim and to forgive in this case.

8.6. **Explicit acknowledgement of arbitrage error.** In a similar way, the arbiter may have to say something about the decision which influences forgiving. This may happen, in particular, if he has found that he has made an error: Or the promise has not been broken, or there was no sufficient proof of this, or the payment of the penalty has been made but was not received correctly because of a wrong account number.

Here, similarly, remains the theoretical possibility of blackmailing the arbiter, which is not very plausible. So one would usually ignore records with such corrections as well. Or, in case the penalty was justified but too large, one would use the modified penalty to evaluate the seriousness of the broken promise.

9. Personal identification control

The network can be used by everybody. Moreover, it can be used pseudonymously. This is a necessity in a statist environment, where powerful criminal organizations can misuse personal information in often unpredictable ways. So, for simple reasons of personal security, everybody should decide himself about the amount of information he gives about himself.

On the other hand, there is a special problem of trust related with pure pseudonymous accounts. The problem is that black list records are much less harmful for such accounts: Everybody can create many different of them. If breaking a promise gives sufficient profit, they have a much higher incentive to take this profit – all they loose is the reputation of a single account out of possibly many. So there will be much less trust into such pseudonymous accounts.

How can this problem be solved? How one can add reputation to an pseudonymous account without giving everybody access to the own private data? One solution is to give the personal information about yourself to a trusted agency. For simplicity, we will assume here that it is simply the arbiter. The arbiter is obliged to hide this information, except for a single case – if the account appears on the black list. In this case, he is obliged to publish the personal data of the rule-breaker. (The "obliged" means, of course, that he accepts this obligation himself.)

But the job of collection and control of the personal data would be better left to an independent external agency. This agency may be completely separated from the network. Its job would be to collect and control personal data and to allow other people to access these data if they can present a key for them. The keys for various parts of the data are, then, given to the owner of the data. So, the arbiter does not have to manage personal data himself, but only the relevant keys for them.

9.1. **External personal identification agencies.** Let's consider at first the external agencies for personal identification.

Their job is to receive various information about their clients, however detailed. They will collect, for example, fingerprints, genetic fingerprints, iris scans, biometric information, verified copies of personal documents – that means, information which can be given during a personal visit to the agency. But it may contain even much less, in particular only information which can be send by electronic mail: Name, birthday, snail mail address, phone and fax numbers, a few personal fotos and scans of personal documents.

As an agency which will have to survive in a libertarian world, this agency has to take into account the wishes of their customers. So it does not require from everybody the same amount of information. It remains the free decision of every client to decide which information he agrees to give to the agency.

Then, the agency and the client will also find an agreement about the amount of testing the information. For example, you can give some information about phone numbers and snail mail addresses to the agency by email. Then, the agency may test them by sending some information, for example a number. The client, then, has to tell the agency this number by email.

Of course, the certainty of the data may be improved very much by a personal visit to such an agency. In this case, workers from the agency can have a personal look at passports and other documents, take personal fotos and the various types of fingerprints.

9.1.1. *Avoidance of doubles.* One thing the personal identification agency may want to check is if there are doubles in their record – people with two or more identities. If there is sufficient information, say, inclusive fingerprints, this could be checked. But one is not obliged to give fingerprints. You decide yourself about the information you give to the agency.

On the other hand, if you give sufficient information, like fingerprints or iris scans, the agency can establish that you don't have doubles among those who provide the same information. This is an important information which increases the degree of security of the data.

9.1.2. *Degree of security of the data.* So, the agency receives various personal information, makes various checks of the accuracy of the information, and finally assigns some degree of security or certainty to the data. This degree will be the highest one

if one gives all the fingerprints, iris scans, genetic material and so on and allows to check that these data are unique. The degree of security will be much lower if the only personal data received are some cell phone numbers and a copy of the passport by email.

9.1.3. *Keys to access the information.* After this, the client receives a unique personal key, to be hidden. This personal key allows to access all the information and to support the information with new data, say, a new address.

The personal key allows the client to obtain some other keys from the agency, keys which can be given to others or published. They give read access for various parts of the information. The minimal information would be a personal identification number, which gives only one information: There is a record with this number in the database of the agency. And there will be other keys which allow access to more information, say, the usual passport data, or even to all the information.

We can also assume that the agency has internet access which also allows connection with pseudonymous remailer networks. Then, the people can use the agency in a simple way – they send a read access key to the agency and receive the corresponding information from the agency.

9.1.4. *Applications outside the network.* A travel agency today, or any other agency which has clients from all over the world, has to accept today passports of a lot of different states for personal identification. This is problematic for the agency, because it does not have sufficient knowledge about foreign passports. So it cannot distinguish faked passports from true passports. Usually this is not problematic. I would guess faked passports are simply too expensive to burn them by cheating a simple travel agency. Nonetheless, this is a risk, and the personal identification agency will be a reasonable way to reduce this risk. Firms with international clients may ask their clients for such an identification number instead of a foreign passport.

Thus, our external personal identification agency will have an independent legal business outside the network, without any connection with the network. There is, therefore, not much to object from the side of the state against such agencies. Of course, they provide a service provided today by states – the identification of citizens of the state outside the boundaries of its jurisdiction. So one may be afraid that states object against a violation of their monopoly. But states have a monopoly only inside their own territory. Which documents their citizens use outside their jurisdiction is not really their business. So, if travel agencies prefer the data from a personal agency in comparison with foreign passports, there will be not much reason to object.

In fact, if such personal identification agencies start their business, one can expect that at least some states will not only allow them to work, but will even force foreign visitors to use them. Last but not least, it simplifies the job of the own policemen – they don't have to be able to handle foreign passports in their jobs.

One may ask why a libertarian, an enemy of the state, proposes to develop agencies which may become even helpful for the state, simplifying the control of foreigners? A good question. The point is that personal identification is an important service, which remains important in a libertarian world too. And the agencies, as proposed here, can and will do this job, and, as usual, in a much better way than the government monopolies. But, of course, every technology has the problem that it may be misused. Therefore it is not strange or unexpected that the libertarian

technology for personal identification, with its advantages in comparison with state monopolies, may be misused by states to control foreigners.

Whatever, the fact remains that such external personal identification agencies – the agencies which will manage personal identification in a libertarian world – are useful even outside the network and can be completely separated from the network itself. This separation may allow them to continue their existence in case of an attack of the state against the network. As we will see below, the network will use the service of these agencies, but so what? There are other users as well, and nobody who provides whatever service can be sure that the service will not be used by criminals too.

9.1.5. *No sensitive information.* It should be noted that the external personal identification agency does not have any information which is in itself dangerous for the participants of the network. In particular, the agency itself does not have any access to the pseudonyms in the network which use their services. If the police obtains all the information about you which is known to the agency, it does not have much – essentially, it has only the information which it can obtain by simply coming home to you and taking all the data by force. In this sense, it makes no sense for the police to take any data from the agency.

Instead, because it is known that other criminal organizations (like the mafia or foreign secret services) would like to have access this information, the state may even prefer to give protection to the security of these data. And even if the secret services would have access to the data, this would be sufficiently harmless. Even if you plan to work as a spy against a foreign state based on a false identity, all you have to do is not to leave there your fingerprints.

9.2. **Placing the personal identification key.** Next, there should be a place where the personal identification key is stored. The natural place is an arbiter accepted by the person – it is he who decides about the record in the black list, so it is he who needs it, and, moreover, he is personally trusted anyway by the owner of the key anyway. Moreover, using arbiters for the placement of this sensitive information gives a warranty that a leak of information is not too dangerous for the network as a whole – only those who have trusted a particular arbiter have to pay for their unjustified trust.

In exchange for the personal key of the external agency, the arbiter returns a signed confirmation that he has received the personal identification key of the external agency AAA from account XXX, and that he has checked that the key is valid, contains personal data of security level X, and that he promises to open this information in the case that the account XXX appears on the black list, and that he promises to check upon request that there is no record on the black list of another account of the same person, and, in the case that such a record exists, to add the information that the account XXX belongs to the same person.

For the arbiter, to check the black list for such records is no work at all, because this will be automatized. If the check gives no result, a corresponding confirmation will be send automatically to the account owner, who can, in a similar automatic way, make this actual result visible to everybody.

We will name an account which provides this information a *personal account*. Those who don't provide this information we will name *pure pseudonymous accounts*. Their owner is completely hidden, and cannot be established by any means, even if he breaks his promises.

10. Controlling the number of pseudonyms

With the methods of personal identification discussed in section 9 one can distinguish personal accounts, with personal information available to the arbiters, from pure pseudonymous accounts without such information. We can be even sure that, if a real person appears once on the black list, all their pseudonyms will be opened too.

But there remains a problem with too many pseudonyms of the same person: They may fake a network of different people trusting each other very much, creating in this way faked reputations.

Is there a possibility of control of the number of pseudonyms, so that their use to create fakes networks of trust becomes impossible? We want to present here some possibilities to manage this problem.

10.1. **The global pseudonym counter.** The pseudonym counter is a monopolistic agency. This does not mean that there is a legal monopoly such that no one is allowed to compete. But it is a natural monopoly in the sense that it becomes a more useful tool if all use the same provider of this service.

Let's see how it works. It is assumed that one of the services of the external personal identification agency is that it gives a minimal key, which is unique and allows to access only the minimal information that there is an account in the agency:

- You start with registering one account – say, your open account – by sending the pseudonym counter the following information: 1.) the identifier of your account in the network, 2.) a unique minimal access key for the data of the external personal identification agency, and 3.) the confirmation of your arbiter that he has received the maximal access key of the agency which correspond to the given minimal access key.
- The counter returns a signed confirmation that 1.) there is no previous record with the same minimal access key, 2.) that your account will be acknowledged as the owner of this key, and 3.) that the data which correspond to the given minimal access key are known by your arbiter.
- You can also register a pseudonym. In this case, you have to provide the same information.
- The counter confirms that he has received the information, and that there exist another account who owns this key, and that the pseudonym in question has the number n in the list of the pseudonyms of this account in the order of their registration.
- The owner can request to close the list of pseudonyms. After this, no new pseudonym of the same person can be registered. It is not possible to reopen it again.

Assume now that there is some monopolistic pseudonym counter agency. Now, you want to evaluate the reputation of a pseudonym given some support for its reputation by other accounts (say, by giving guarantees, as discussed in sec.).

Naturally, you want to know how many different persons are behind these personal pseudonyms. For this, it is sufficient to compute the maximal number of pseudonyms with the same counter number. So, if there are, for example, four basic accounts (number 0) and six first pseudonyms (number 1), this maximal number is six, so at least six out of the ten people who have given guarantees are different real people.

So, to create a network of your own pseudonyms is no longer meaningful: They can be easily identified, or by their high pseudonym numbers, or by not giving such numbers at all. All the people supporting you would have to have different numbers and, therefore, the algorithm would tell that only that it is at least one person who has given support – and possibly not even one different from the pseudonym itself.

10.2. **Is the counter-monopoly dangerous?** Monopolies are dangerous by default. Whenever we have a monopoly, it seems reasonable to think about the possible dangers. So let's see.

A first point is that the monopoly receives only information by those who trust it. And all it can do is to misuse this trust and to give the information about the pseudonyms to other people. There is no way to misuse the data in other ways: The keys which would give access to the real data of other people are not accessible to the agency – it receives only the minimal keys and confirmations from arbiters.

The only thing he can do is to create a fake network of own pseudonyms and assign them – falsely – that they all are the first on their lists of pseudonyms. But if one of them fails and appears on the black list, the fake becomes obvious – the methods of section 9 will be sufficient, and one can find, then, that all the pseudonyms of the same person have been the first pseudonyms in the same pseudonym-counter agency. After this, the agency is finished. So this would be a quite stupid idea for misuse.

To make a lot of money out of the monopoly would be, of course, possible. In a state where the network has been forbidden, it would be interesting for the police to learn who of the formerly open accounts continues to use the network with pseudonyms. So they would like to have access to these data, and, possibly, offer a lot of money for them. But I think there are a lot of people in the world who would reject such offers. Maybe because they are already rich enough, maybe because they have own illegal interests which would be endangered if the network will be harmed, maybe because they hate the state or simply because they are honest. Or, last but not least, he may be simply afraid of the black list. In fact, it would be impossible to obtain a monopoly without having submitted his personal data to several highly trusted arbiters, and without accepting the black list plus death penalty for selling the data. Whatever the reason, if there is one such agency which does not sell the data, this will be the one who becomes the monopolist.

Then, the information itself is not that problematic – it is not even the information about the real person behind a pseudonym, only the information which pseudonyms belong to the same person. There are other police methods which allow to establish such correspondences: A sufficiently large number of texts allows to do statistics about the errors.

In fact, the information the agency really has to store is not even interesting for the police. It is sufficient to store only the following data: 1.) The minimal key, 2.) the owner, 3.) in case of an open list, the actual number of pseudonyms, in case of a closed list the information that the list is closed. Of course, the open source

software for this program will store only this information, nothing else. So, whose who would like to sell data to the police would have to have this intention from the start.

Another point is that, even if the monopoly is a natural one (that means, the more people use the same agency, the more useful it becomes to use it too), it can be easily changed. Indeed, one needs almost nothing to start a competing business – start an open source program on a server hidden in a darknet. And all it needs to destroy the old monopoly is a loss of trust.

This makes it impossible to misuse the monopoly as the state does – to enforce other monopolies in other domains. If the monopolist behaves in a way which is not nice, another will easily replace him, and behave in a more civilized way.

10.3. **What happens if the state forbids the network.** So what happens if the state forbids its citizens to use the network?

You have been an open user of the network before, and also, officially, a law-abiding citizen. The last thing you do as long as the network is legal is 1.) to start a record with your first, open account, 2.) to create a few pseudonyms, and 3.) to close the list of pseudonyms.

Once you have done this, what can the police do, given the fact that it knows about your previously open account?

- In general, there will be no possibility to close network accounts. Once created, the account remains an account. Once there is no such possibility, the police cannot blame you for not closing the account. And, of course, also not for having an account, created at a time it was yet legal to do such things.
- But there may be some police spies in the network who can report if your open account shows any activity. So, using the account during the time of illegality would be dangerous. But that's why you have created your pseudonyms.
- The police can suspect that you have pseudonyms. The police coming home to you can aks you to present the information from the known account. The information tells the police that your record is the first in the list, and that the list is closed. That means, the information is the same as in the case where you have not created any pseudonyms.
- The police may wonder why you have created such a list at all. The answer is straightforward – to prevent other people, who may have obtained access to your key from the personal identification agency, to misuse this key for creating fake identities. And, that's why, you have closed the list.
- If you would not have closed the list, the police could force you to create a new pseudonym and to put it into the list. In this case, the information about the pseudonym – that it is pseudonym number n in the list – would give the police information about the number of your pseudonyms. So you could be forced to open all other pseudonyms to the police. The possibility to close the record once and forever (else, you could be forced to reopen it) is therefore a safety device.
- To give information only about the place in the list, instead of the number of pseudonyms, has the same aim – to protect you. You can claim that you have not created any pseudonyms. And the only way for the police to

learn that in fact you have created and used pseudonyms is if one of your pseudonyms breaks a promise and appears on the black list.

So, you can use your pseudonyms, and for each pseudonym there is, visible for everybody, the information that there is a known real person behind it, and that the pseudonym has number n in the list of pseudonyms.

This is already information sufficient to establish personal trust based on the identity. Of course, if you know that the pseudonym is the second in the list, you can guess that the first one is the open account which cannot be used in the current circumstances. But you don't know yet if there are some thousands of other pseudonyms. But this is not a problem, because the other pseudonyms, if they exist at all, have higher numbers and, therefore, will be more suspect. A pseudonym with ordering number 783 will not be trusted much.

11. Guarantees

There is another interesting way to improve the trustworthiness of an account, open or pseudonym, which could be named bail, guarantee or suretyship. I will use here guarantee. It is a limited guarantee. If the guy who receives it appears on the black list, you have to pay his victim the amount specified in the guarantee.

There is a quite natural way to obtain such guarantees. If you have cooperated with somebody in a successful way, and have obtained by this cooperation some profit, why not give him a guarantee over some part of the profit, in exchange for a similar guarantee? Your risk is small – you have had some positive experience with him, thus, some reason to trust. And even if you have to pay, some of the profit you have made in the cooperation remains. On the other hand, you receive a guarantee, which increases your reputation.

If guarantees are given in this spirit, there possibly will be a lot of them. So it seems reasonable to automatize their handling: If somebody appears on the black list, the arbiter will automatically send all those who have signed guarantees an information about the necessity for payment. Everything in this information can be checked automatically, so one will make these payments automatically too.

If no payment is made, this may be established automatically too: The guarantee will contain a maximal time delay between receival of the information and payment, and if there is no payment made after this time, one will end almost automatically on the black list.

It seems even reasonable to create, for this purpose, some automatic arbiters: Everything they have to establish can be established in a completely automatical way – the justification for the payment request as well as the non-payment after the established delay for payment. So, non-payers may appear automatically on the black list.

11.1. **Faked guarantees.** How one can misuse guarantees to cheat? One may think about exchanging with completely unknown people large guarantees. But this would be unreasonably dangerous. You could easily be forced to pay them. So this seems reasonable only if you plan to cheat and to burn the pseudonym in short time, so that your pseudonym burns before the other one, and, in case that you have to pay, not to pay but to throw the pseudonym away. So you will do this only with pure pseudonyms, where you don't have anything to loose. The other side probably thinks similarly, so the question is who succeeds to cheat before the other.

Above pseudonyms will not last long, and will not really obtain a good reputation: The very combination of large guarantees by pure pseudonyms will be considered as suspect.

So this method will not work. Moreover, there is a much safer way – to create several pseudonyms yourself and exchange guarantees with yourself. This may result in a faked subnetwork where everybody trusts each other very much, offering high guarantees, where in fact the whole network is created by a single person.

Given these possibilities, the problem is how to evaluate what the guarantees are worth. This job has to be done, of course, by programs. These programs may have quite sophisticated strategies to evaluate the reliability of all the presented guarantees. So let's consider some ideas used by such evaluation programs.

A first idea would be to distinguish persons by their personal identifications. An open account will have the highest value. Next, there will be pseudonyms backed up with personal information. Their reliability depends, of course, on their position in the list of pseudonyms. Pure pseudonyms, without any personal information behind them, will not be trusted.

This does not mean that guarantees given by pure pseudonyms are completely worthless. Instead, one may look at those who support them with guarantees. If among them are more trustworthy pseudonyms, fine. One may even evaluate third or forth order guarantees. This is reasonable once not only payment of guarantees but also the appearance of non-payers on the black list is almost automatized. In this case, the second order guarantees have to pay. And so on. In fact, a whole faked network can be destroyed in this way.

Having a whole network of pure pseudonyms does not give much, because it may be faked by a single person. So, what a program has to look for is if there are real persons behind at least some of those who would have to pay. If there is a real person behind it, one can imagine that it does not want to appear on the black list for not paying a small amount of money. How much is another question – this everybody has to decide for himself.

So, based on the assumption that a real person will prefer to pay some amount of money instead of appearing on the black list, one can compute the value of a guarantee which is part of a network of guarantees between pure pseudonyms, pseudonyms backed up by personal data, and open accounts. If there are, for example, three open accounts (number 1 of their pseudonym list) and four first pseudonyms (number 2 of their list) one knows that there are at least four real persons involved.

11.2. **Strategies to obtain guarantees.** In the case where the network is illegal only in a part of the world, where is a way to obtain guarantees from real people – contact with real people outside, where the network is legal. In the simplest case, you put your money on a bank account in the free part and obtain, in exchange, a corresponding guarantee. (There will be, of course, also possbilities for guarantees given for some fixed period of time, so that one is free, after this, to take the money back.)

The same technique works also if there is a trusted network bank inside the state.

Having a sufficient initial reputation backed up by own money on a bank account may be a reasonable starting point for creating reputation by providing adequate services for customers.

The second way to obtain guarantees is cooperation which is acknowledged after the fact as successful. Then, the increased reputation of the participants for each other may be backed up by guarantees given to each other. The amount does not have to be high – a lot of good cooperation with resulting small amounts of guarantees gives also a high amount.

A problem appears if the cooperation is done based only on pure pseudonyms. This would be preferable in a situation where one wants to do something seriously illegal. But if there are only guarantees given by pure pseudonyms this does not give much reputation. Or, more accurate, the additional reputation would be restricted to those who assign, because of personal knowledge, high reputation even to the pure pseudonym.

But one can apply in this case a strategy of minimization of possible harm.

First, you create a personal pseudonym. For security reasons, you do not want to start doing really illegal things with it in the network. Instead, you use it for only one purpose: To give guarantees to the various guys you really trust. So, to find customers and cooperators you use a pure pseudonym. You can give this pseudonym, for the start, some guarantee from your personal pseudonym. Then, if you cooperate successfully, you can offer your cooperator a guarantee from your personal pseudonym, in exchange for a similar guarantee from his personal pseudonym. After this, your trusted cooperator now knows your personal pseudonym, but this does not give him much dangerous information too – that you are doing really illegal things he already knows.

On the other hand, if the police establishes the identity of your personal pseudonym (say, because the pseudonym counter agency was a police trap) they can find out that you have done something forbidden – you have actively participated in the network during the time where it was already forbidden, by giving guarantees to various pseudonyms. So one can expect that this will be penalized, but not too harsh, so that the harm is not that serious.

In this way, you can also obtain guarantees for your pure pseudonym given by pseudonyms with personal identification.

11.3. **Higher order guarantees.** But even guarantees given by pure pseudonyms are certainly not worthless. There may be other reasons to trust.

There is, for example, the factor of time. Guarantees given long ago are worth more. Then even pure pseudonyms may have high personal reputations among those who have had personal contact with it. Unfortunately, this is a point which cannot be estimated by a program. (Or, more accurate, I do not see a sufficiently safe way for doing it.)

But the pure pseudonym may have received guarantees by other people. The very point is that for not paying the guarantee you end on the black list, and in a quite automatical way. So, if one evaluates the guarantees one can look for such second order guarantees. Or for third order guarantees. How many different people are behind them? This is something which can be evaluated by a program again.

One will, of course, look for the different pseudonyms who have given these guarantees, to see how many people are behind them. If all of them are unbacked, they may be created out of nothing, a fake network of pseudonyms giving each other guarantees, created by a single person.

11.4. **Not too complex?** All these mechanisms seem extremely complicate at a first look. Maybe they are far too complex? Maybe personal networks, based on personal trust established by personal meetings, is a much more secure way to establish trustworthiness?

I don't think so. First, things which look complicate if described here may appear much less complicate in reality. In fact, the problems I have described are mainly the problems of writing software which automatically evaluates the reputation of a person. So, the user of the network does not even recognize them – he simply uses software written by others. It is necessary to find out if there are valid and reasonable algorithms for doing the job.

Then, the newbie does not need them all at once. He starts with a simple, pure pseudonymous account and learns to use all the things which can be done without any own reputation. For example, he can participate in really uncensored discussions in various forums, exchange files in a really safe way, open a network-internal bank account, and then to start to buy or sell something. At first, without own reputation, he has to pay or deliver in advance. This is something one does not like, so he wants to learn how to improve his reputation.

Let's simply compare how, say, an illegal internet-based networks can be created today. One starts with an open forum, where people talk about something related with the illegal activity in question. You may find there somebody with common interests. He may invite you into another, already private forum, where more people sharing your illegal interests communicate. After some communication in this forum, people form an opinion about you, and if some have a positive opinion about you, they may communicate with you personally, and, later, invite you to a personal meeting. If the illegal business starts, depends on the results of such meetings. So, the decision is usually based on some communication through the network, and, after this, on some personal communication. Of course, there are people who have sufficiently good intuitions so that they can make reasonable decisions based on such information. But it is, of course, quite easy to contact, in this way, undercover policemen or journalists or other despised persons.

The very point of the network is that one has, now, much more information. The most important one – that there is no record on the black list. And even if the personal data are not known, because a pseudonym is used, the information available through the network allows to establish much more.

In fact, people learn such things easily. As they have learned, after the fall of communism, to live in a world where prices are no longer fixed, and where one can sell and buy what one likes (not completely, but with much more freedom than before), they will learn what can be done in the network.

12. Defense against attacks by the state

The government may not like the network idea. There are a lot of reasons for such negative feelings. In particular, the network may be used for a safer organization of illegal markets. Moreover, a network-internal banking system provides a lot of possibilities for tax evasion. The danger of corruption increases too. All these are things unfavourable for the state.

But there is no necessity that the state will fight. There are even some circumstances which may prevent him from fighting. A particular interesting one is that the network is especially interesting for the rich and powerful. They have much

more to hide from taxation. They have much more to win by corruption. They are clever enough to recognize the advantages of the network. So it may happen that the elite is much earlier part of the network than the rest of the population. Now, one may think that the preservation of the state is in the interest of the elite. But, first, it is in fact not, at least not that much as one may think. Then, the interest of preservation of the state is a common good (or evil). The personal gain from participating in the network is, instead, a private good. Once people care more about their private goods, the elite will not care that much about the state as one might think.

Whatever – there is at least a danger that the state will try to fight the network. The network has to be prepared for this case. Here are some ideas how the network may be defended.

12.1. **The legal case in favour of the network.** The basic things which can be done in the network are things which cannot be easily forbidden without endangering the very foundations of democracy and freedom of speech. Indeed, let's look at the details:

First, people propose laws which they accept as just. But this is a necessary part of every democratic society: People make proposals how to change the laws, and argue in favour of them. If one forbids the people to make proposals for better laws, the state cannot be called a democracy anymore. The right to make proposals for better laws is fundamental, constitutional for a democracy. So to defend this part is really easy.

But one also promises to follow the laws one has proposed. Here, it may be argued that this can be forbidden. But this is completely unjustified. In the worst case, one can simply replace text like "I promise to follow the following rules: ..." by a more harmless text like "I consider the following rules as just and acceptable and would promise to follow them if they become accepted as laws by the state: ...". Anyway, to promise to follow rules which are not laws of the state is something we do a lot of time: If we become members of organizations, if we sign contracts, if we accept religious beliefs.

The state may object against particular rules directed against the state, like rules of type]"I promise not to tell the police about ...". But this can be easily avoided. Instead of the police, it suffices to mention members of criminal organizations. It seems almost impossible to object against such a promise. Of course, the criminal organizations are defined as organization which do not accept the Golden Rule, so that the state is included.

Anyway, the promise to follow the own general rules will be in almost all cases legal, simply because one is usually not obliged to call the police if one knows about some crime. Thus, exceptions will be only relevant for a small minority of participants. Instead, the contracts between the participants will be private, not accessible to the public.

Then, there is the acceptance of arbiters as trustworthy. What could be wrong with this? It is beyond my recognition.

Then, the arbiters are simply expressing their personal opinion about some real fact. They try their best to tell only the truth. Moreover, those who will be victimized by the particular records about their behaviour have signed an explicit agreement, so that they have no moral right to object. So what would be the

justification for the state to object here? Certainly not that lies are distributed. This may happen, but these will be a rare, unintended exception.

One could object that the record contain facts about the real contracts which have been broken, contracts which may be quite criminal. But there is no necessity for this. As considered in section 8.3, the information one needs is not the complete one in all details. In a situation where the state exists and may harm the victim for signing the broken contract, it would be stupid to provide such information. And it is not necessary at all, because the details about the broken promise will be decided in the first round. This first round establishes a penalty. The record in the black list is only about the failure to accept the penalty. This is all the information one needs: There was an earlier decision by the arbiter, which is hidden to protect the privacy of the victim, but which has established a penalty X. The contract breaker has not accepted it (is running away, not paying etc.). Date, signature of the arbiter, signature of acceptance of the arbiter by the contract breaker, point. All this is quite neutral information, which in no way suggests that the broken contract was possibly a criminal one.

So the key elements of the network are extremely hard to challenge. One would have to restrict the freedom to propose better laws, or the freedom to promise to follow some rules, or the freedom to tell that one considers somebody else as trustworthy, or the right to tell a truth about somebody even with his prior agreement. If all this remains legal, everything one needs to evaluate the reputation of a member is available.

But this is all one needs for the network to have its independent value. All other parts, in particular the internal banking system, may be outsourced, organized separately. If in these other parts something criminal happens, this is nothing the network itself has to care about.

12.2. **Ghandi-like open violation of anti-network laws.** Given this argumentative situation, it seems not unrealistic to develop a sufficiently strong movement in support of the legality the network. And, in case of a law which forbids the network, one can try to use the strategy used by Ghandi – open, demonstrative violation of the law, with open information of the police about this fact.

It depends on the number of network members who agree to participate if such a strategy may become successful. But I don't think one needs very large numbers of participants. Then, they probably do not risk very much – at least initially the penalties will be sufficiently small.

By the way, it would be very funny to have some obviously harmless participants who accept the actual laws of the state as they are (except for this single one which forbids to tell about this), and accept the courts of the state as they are as just arbiters.

Of course, some minimal number of participants is necessary to reach the aim. But it seems to me that it is not the number which decides the question, but the very argumentation in favour of the legality of the network as discussed above, as well as the very aim of the network – to allow people to establish a reputation for honesty. Honesty is a virtue, not a vice. People who have this virtue should be allowed to prove this, to obtain reputation for their honesty.

To go into prison to be allowed to prove the own honesty is an interesting and attractive challenge for all those fascinated by peaceful movements like Ghandi's. So it seems not unreasonable to hope for a success of such a movement.

But assume this movement fails. What can be done? This, obviously, depends on the restrictions applied by the state against the network.

12.3. **If the internet itself is closed.** In the worst, totalitarian case, the internet itself will be forbidden. This seems not very realistic, because it would be already a large loss for almost everybody. So to find a democratic majority to forbid the internet itself seems hopeless almost everywhere.

If this happens, all one has to do is to emigrate and to wait. It is reasonable to hope that one has to wait much less time than the Russian emigrants for the end of the communist regime.

12.4. **If strong encryption is illegal.** A more realistic and therefore more dangerous proposal is to forbid the use of strong encryption. Encryption will be allowed only with a backdoor for the police.

In this case, there are different strategies of defense. First of all, one can use strong encryption inside and weak government encryption outside. If the state needs at least some formal justification to be allowed to use the backdoor, this gives already a partial defense. In the worst case, one has violated the law against strong encryption.

Another method is steganography. The idea is to hide encrypted information in unimportant, appropriately manipulated bits of pictures, videos and other legal files. Here, the police has a much harder job to detect that illegal encryption has been used.

12.5. **A friendly virus: What to do if particular programs are forbidden.** Assume the use of some program is forbidden in a state which is not completely totalitarian. In this case, there is a quite simple strategy: To implement the illegal program as a "friendly virus". The friendly virus behaves like a virus – it infects programs. If the infected program is used as usual, it behaves like the original, uninfected program until it receives some text input. Then, if the text input is identical with a password known by the user, it starts to work as the illegal program. If not, the user will not see any difference between the original program and the infected one. But in fact something different happens: The virus tries to distribute himself, and, additionally, also does things which emulate the use of the illegal program.

The programs used by the network will all be based on strong encryption, so the emulation consists in behaviour like creating encrypted files or sending them through the internet. So, what the police is able to detect is the following: All the usual traces which can be used to identify users of the illegal program, like encrypted data, or internet communications with the exchange of encrypted data, are present. And the illegal program itself is present too, as a virus.

But there will be no chance to detect the difference between the faked behaviour by the virus and the real behaviour of the user who knows about the virus and knows the password. The reason is that all the detectable traces consist of encrypted information. Without the key necessary for decryption they have nothing.

So how to distinguish the innocent victim of a virus infection from the criminal user of the program? This seems close to impossible a posteriori. One would have to observe what the user is really doing all the time. This is not impossible, one can, for example, hack the computer and install there observational software like keyloggers, or break into the private rooms and install there hidden cameras. But

if the virus becomes quite distributed, this would mean that such measures have to be applied against a lot of completely innocent victims of the virus infection. So the state has to be already quite totalitarian to be able to enforce such a law.

12.6. **Surviving with strong encryption.** Let's finish with the easy part – how to survive if strong encruption and internet connections remain possible. This does not mean that they have to be legal – it is sufficient if the countermeasures described above, or some other measures, appear sufficient or the enforcement of anti-encryption laws is inefficient for other, unknown, reasons.

Once encryption is possible, it can be used to hide the parts of the network which would be open in a legal situation too. But this would not be sufficient protection: Last but not least, most of the information would be open to every participant in the network, and nobody prevents the police from participating.

So, if the network is illegal, the participants would be forced to use pseudonyms to hide their identities. For this reason alone, it seems useful to allow pseudonymous accounts in general from the start.

13. A legal network in a statist society

The network can be created today. All one needs is appropriate software – something we can start to implement today – and the internet, which already exists. There are even subnetworks like Tor or freenet which make control by government much harder (if not almost impossible).

Once it is implemented, one needs people who try it. They will find out the weak places and improve it. Initially, there will be only a few participants. This situation may be the critical one, because the network becomes useful and powerful only with many participants. But I don't think there is much reason to be afraid. That's because there are some simple applications of the network which make the network attractive even for small groups. We will consider some examples below.

What follows is an already sufficiently large network in numbers, but yet small in comparison with the whole population. Say, some hundreds of thousands in a single state, or millions over the whole world. In this situation, the network becomes more and more useful for its members. And, as a consequence, the black list becomes more and more dangerous as a penalty. You have yet all possibilities to live outside the network, but the blacklist record becomes already a loss. Moreover, the black list is visible even to non-members, so they may use it too.

Once this state has been reached, the attractiveness of the network has a potential to increase. There will be jobs offered only to members of the network – this becomes attractive, because networkers are more reliable and will not use the expensive and unreliable government courts in case of conflict. First this will be mainly the black job market, in particular jobs where contracts cannot be enforced in government courts because some points are forbidden by one or another type of government regulation. Then it will cover contracts where government courts are problematic for other reasons, for example, international contracts. But finally people will prefer volitional arbitrage simply because of higher reliability and lower costs in money and time. But to use this method of arbitrage requires, of course, membership in the network. Once network members will be preferred on the job market, people will become members simply because they want to find good jobs.

13.1. **The internal banking system.** Once the network is large enough, an internal banking system will start to work. There is not much one needs for this. The appropriate banking software will be part of the network software anyway. To increase security, safety, and anonymity, appropriate transfer protocols like ecash will be used. Bankers may be simply trustworthy persons who manage the software. Only from time to time, in case you need cash or have to pay, they have to organize transfers between your internal account and your external banking account. This may be, for example, done by a transfer between their external bank accounts and your external bank account.

One great advantage of such an internal banking system is that the state cannot control it. All information which the state can obtain is that there are a lot of small transfers between the external banking account of the banker and your external banking account. This is not much – it is used only if you really need cash. And it also gives not much information about the nature of the income. Of course, there will be also transfers between different bankers. But there will be a lot of internal clearing which never leads to traces in external, state-controlled bank accounts. And the larger the network, the greater the role of internal, undetectable circulation.

Each internal transfer is a possible tax economy: A pays to B. In many jurisdictions, this is an income for B which has to be taxed. But if B does not declare this, and the state is unable to identify this, it cannot be taxed. As a consequence, the internal banking system creates a lot of possibilities for tax avoidance. This starts with black market jobs and does not end with tax-free payments for whatever you like. The main point is that the government has no longer any information about your real income.

13.2. **The special attractiveness of the network for the rich and powerful.** Given the heavy progressive income taxation in many states, the network becomes especially attractive for the rich and powerful, or, in other words, for the ruling elite.

The avoidance of the progressive income tax is not the only point which makes the network especially attractive for the rich. One should not underestimate the criminal energy and corruption among the ruling class. For the management of various non-legal payments the network will be a nice possibility. As a consequence, one has to expect an increase of corruption in the states in general. Indeed, the network increases the safety of corruption: Payments are made by reliable network members, which can be much better distinguished from undercover cops. Then, payments will be made not in real cash, or via state-controlled bank accounts, but via the network-internal banking system, so that it leaves no trace on legal bank accounts. It seems not unrealistic to think that corruption is more distributed among the rich and powerful, so, as a consequence, the network becomes even more attractive to the rich. Because of the increase of safety of corruption it becomes attractive for the corrupt government workers, which are, in the average, also powerful people (it is, last but not least, their power which forces others to pay them bribes).

What will be the outcome of increasing corruption is a difficult and complex question, but one of the results is surely the decrease of the income of the state itself (if instead of taxes you pay bribes to government officials) and the decreasing ability of the state to use this income purposeful, in particular for fighting the

network (if you bribe policemen for not enforcing some laws, or state property is sold for cheap to private persons).

These effects are likely to decrease the resistance of the state in its fight against the network. First, with the loss of a lot of tax income and increasing corruption the ability of the state to fight decreases. But even more important is if the ruling elite itself is participating in the network. The ruling elite certainly will not fight itself. Given the special attractiveness for the rich, one can imagine a situation where the ruling elite is already part of the network, but the man on the street hasn't even heard about it. In such a situation it is unlikely that the ruling elites will focus the interest of everbody on the network by fighting it.

The special attractiveness for the already rich and powerful is a point similar to the situation in communist states before 1989. To open the society was especially attractive for the ruling class – those who have become the superrich in these states after privatization. The times have been hard for the large masses of poor people, but much more attractive for the winners of the privatization, for those with connections with the establishment. This special attractiveness for the ruling class may have been one of the main reasons why the anti-communist revolutions, with minor small exceptions, have been peaceful.

Of course, one cannot exclude that there will be sufficiently strong forces inside the government which want to fight the network. Last but not least, the network is dangerous for the very existence of the state, and therefore for their own power base. But, on the other hand, the survival of the state will be only a common good of the whole ruling class. Instead, the advantages they obtain from participating in the network are their private goods. Standard economic theory teaches us that most of them will care more about their private goods. In particular, cheating the state in favour of a private company can give a large enough income so that a possible future loss of this possibility is not that dangerous.

Thus, one can hope as well that the special attractiveness of the network for the rich and powerful will be helpful for a peaceful transition into a libertarian society.

13.3. **The raise of illegal markets.** With the increasing importance of the network, one of the most powerful mechanisms of state power – state courts – loose their importance. Private conflicts will be solved increasingly by volitional arbitrage, outside the system of state courts. But it is not only the number of conflicts solved by state courts which matters. Much more important is their influence – the danger that, in case of conflict, one of the sides will go to a state court decreases: If it is part of the contract not to go to a state court, network members will not react in such a way.

Next, there will be an influence on the power of criminal courts as well. There are two reasons for this. First, the rules used in the network will offer as penalties, instead of jail sentences, payments to the victims. So, for victims it becomes more attractive to ask, at first, private arbiters. It is quite obvious that they will receive their compensation only if they promise not to call state police. So the state will loose a lot of its influence even in cases which today are covered by criminal justice, simply because fines paid to the victims are more attractive for the victims of crimes.

But another mechanism will be much more important for the general weakening of the state – the improvement of the illegal markets. With the network, it will become much harder for the state to fight all those victimless crimes: Restrictions

for gambling, prostitution, pornography, sex, drugs, tobacco and alcohol prohibitions and so on. The entrepreneurs in these domains become more reputable, they have less incentives to cheat given the danger of the black list, and the system of arbitrage gives them more civilized methods of conflict resolution – the age-old problem of illegal businesses. With less violent fighting between different illegal businessmen where is less justification for police intervention.

Then, to become a police informant becomes more dangerous in the network – again, because of the black list. And, again because of the black list, an informant will be successful only once. A life-long job as a police informant becomes impossible. Thus, there will be less informants, and those remaining will be less productive and ask for more as compensation for their higher risk. But informants are a necessary instrument of police control. Without informants, police is almost blind.

Another point is that, with the network, one can use much better and safer ways to find clients. One problem with trading illegal drugs and prostitution is that to find new clients one needs some contact with the general population, which contains a lot of people who feel offended by the offers. Now, advertizing in the network will be more efficient. Reading your rules, one can already see that you will not like some offers. If you describe in your rules that you respect drug laws, only idiots will bother you with proposals to buy illegal drugs. Thus, the illegal markets will become much less offending for those who don't like them, simply because they no longer see them. Citizens offended by illegal proposals are another powerful source of information for the police, so this leads to a further decrease of police power.

To use illegal markets as a customer becomes much safer too. Today, you have to believe an offer given by some unknown, often dangerous-looking person, some of them being undercover cops, or journalists, or blackmailers. In the network, you can search for proposals made by people with well-established reputation. The black list is extremely helpful in this context too. So illegal markets will work much more smoothly. If not completely without the classical problems caused by police restrictions, then at least much better and safer than today.

We have already discussed the increasing possibilities for corruption as well as the advantages of a network-internal banking system. Above points are extremely important for the safety of illegal markets.

All this possibly leads to some increase of illegal markets. As a consequence, an increasing number of people will work in these markets. They have no connection at all with the state – they don't pay income taxes, they don't care about the laws, and they don't cooperate with the police at all, except possibly for payments of bribes. And an increasing number of people will use these markets as customers. Such a raise in illegal markets will have a back-reaction on the network-internal banking system: It increases the network-internal circulation of money and the attractiveness of network-internal payments.

13.4. **Increasing reputation of political prisoners.** A natural change in the evaluation of other people follows. Today we have, outside small networks, almost no information about the reliability of other people. We have to rely, at best, on their empty criminal record. This changes in the network. Here, the black list contains much more interesting information: The information if we can believe his promises. The empty criminal record remains silent about this – it tells only if one likes to violate state laws or not. But this is not the information we really need, in

particular in the case of participants of illegal markets. Reliability is much more important.

As a consequence, people will despise those on the black list much more than those with other criminal records. Those on the black list are the real criminals. Those with other criminal records are those who have violated only unjust laws, laws which they have openly disqualified as unjust, so that their violation is ethically unproblematic. One can disagree with his political or ethical position, but he remains a honest, reputable man even in jail – like a polical prisoner today.

So, the general reputation of all those who violate the laws of states, but not their own rules, increases. They obtain a status similar to that of political prisoners. If they come out of jail, their moral reputation (in the eyes of the network members) has not been damaged by their jail sentence at all.

One may think that such modifications in public opinion are not very important – what counts are the hard facts. That would be wrong. In human relations, such "ideal" things like reputation are extremely important. History teaches that many people have been ready to die to preserve their reputation – to live without reputation would have been worse for them than death. So such a change in the public evaluation of reputations could be extremely important for the fate of the network.

Because of the importance of such a moral shift, let's reconsider the reasons for this shift in more detail. Our main point is to clarify that this shift is a rational one. The participant of the network has rational reasons to prefer the new type of political prisoner in comparison with the true criminal.

Indeed, the main rational reason to think about reputation is the expectation about the his behaviour in some possible future cooperation. It is rational to expect that his previous behaviour will be predictive for his future behaviour too. So we have to think about the question if we can trust him. But this does not depend on his relation to the laws of the state, at least not if he openly names them unjust. Indeed, the situation in a contract with you is different. Once he has signed the contract volitionally, he has acknowledged the contract as just and binding. So if he would break your contract, this would be something new. Instead, if he has already broken a contract or a rule he has accepted as just, the situation is different. You have to expect that he may break your contract too. Thus, it is rational to cooperate with the political prisoner, but not rational to cooperate with the criminal promise breaker.

Then, the part of the reputation which is important is not what you officially claim to think about him. The important part is if you are ready to cooperate, ready to believe him, because it is this cooperation which is useful not only for you, but also for him. So, it is not only rational for you to prefer the political prisoner in comparison with the criminal. It is also rationally preferable for him to become a political prisoner in comparison with becoming a criminal.

The last point is an important one: In case of conflict, people will prefer to hold their promises even if this leads to persecution by the state. If this shift has happened, the power of the state will be reduced essentially: Even legal obligations to call the authorities if illegal behaviour becomes known will fail.

13.5. **Decreasing regulative power of the state.** Another source of power of the state are the various interventions of the state in all domains of economics. Today, such regulations usually have effects. The problem is that in case of conflict

people are used to call the state courts. But these courts will enforce what is prescribed by the state, overruling different choices of the partners in private contracts. So, once people cannot exclude a possible later conflict and its resolution in a state court, they have to be afraid of using illegal clauses in their private contracts.

But with the network, where appeal to a state court can easily be excluded, this becomes much less dangerous. So people will no longer care in their private contracts about regulations by the state if they are in conflict with their own interests.

Thus, the regulative power of the state vanishes or at least heavily decreases. Whenever the state tries to forbid some type of behaviour which is in the interest of all contracting parties, the regulation will be ignored. But it will nonetheless have some consequences: Because the contract contains something illegal, the contracting sides have to insist, as part of the contract, that state courts should not be called for conflict resolution. Once the regulation by the state covers almost everything, from jobs to housing, almost everybody will depend on contracts which explicitly forbid to call the state in case of conflict.

Those who recognize this will accept from the start, as a general rule, that it is unethical to call the state or any other criminal organization in case of conflict. Once people have to insist on such clauses anyway, those who accept such a general clause from the start, and as a consequence in all their contracts automatically, will be preferred. So one can predict that a general rule not to call the police in case of conflict (with violent crime as a possible exception) will be accepted by a lot of participants of the network.

This additionally decreases the power base of the state.

13.6. **Development of a shadow economy.** As long as the state has enough manpower to control a lot of things in real life, the obvious way to minimize taxes is the development of a shadow economy. The things done in real life have to be combined with faked documents in such a way that police has not much chance to establish that there is anything wrong except by very intense and regular controls. For example, the official working contract may be a half-time minimal wage contract. Is there anything to object? Officially not. One needs a lot of control to establish that they in fact work full time or even more, and one has no way to find out that part of the payment is received through the network.

How much does the firm produce? This is not easy to establish. So what is the problem if the official documents reduce the number of items sold by a factor two? Do policemen want to count all the nails? Not? Again, the money for the other half are paid through the network. As a result, the firm does not make any official profit. It officially doesn't produce enough to be able to make it. Whatever the receiving firm does with the shadow items, they will certainly not appear in their official documents. Once they use the same sort of items officially too, the police would have to count them to find out the extra pieces.

You buy some luxery. How much is it worth? You officially pay less, the remaining part is paid in the network. The firm has a lower income to tax, and your property is officially much less worth if there is some property tax. Even counting doesn't help here.

Of course, to pay less in a shop may be difficult – there may be non-members in the shop too, who have to pay the full price. But how to control home delivery?

What can be done by the state against a developed shadow economy? Essentially not very much. One thing would be complete control. Counting nails. It seems, the

costs of this will be far too high in comparison with the gain. Then, you can count things. You cannot evaluate the real market value of them. You can control shops. It is much harder to control home delivery. Those who control will be hated. One has to pay them a lot to motivate them. Those controlled may offer them some payment to demotivate them.

One can increase the taxes. But you cannot tax too much from the minimum wage if you don't want to risk a revolution – those who really receive only minimum wages have not that much to loose. If one increases taxes on profits, the main effect will be that the remaining honest firms will punished. Indeed, however you increase the taxes on profit, you cannot tax in this way a firm which does not make a profit. So, to survive on the market, one has to participate in the shadow economy and therefore in the network – a further increase in the membership, by rich and powerful people.

This leads also to a further shift in the relation to the state. For network members, the state is much less useful – they will not call the cops in most of their conflicts anyway. But cops become more and more dangerous for them – while participation in illegal markets and the shadow economy is much less dangerous than today, all what happens in real life can be, in principle, controlled by the police. So the number of those who have only fear and hate for the police increases. And even the increasing participation of the police in the shadow economy by bribes does not really make the police more popular.

The problem of the government is simply missing information. One can no longer identify the rich, those who can be taxed. And it becomes more and more obvious that the poor have to pay almost all the taxes. Police methods in real life, without sufficient support with information from the population, will give at best proportional taxes, but probably something more close to head taxes.

Whatever, to receive the taxes, the state has to spend much more for control of tax avoidance by the shadow economy. So there remains much less to be spend for other things. So it is quite probable that regulations which do not improve the tax income of the state will be enforced in a less rigorous way, and, possibly, essentially will be given up. This leads to an important improvement for the whole economy.

13.7. **Loss of the power of labor unions.** An increasing difference between legal contracts and de-facto contracts creates a problem for labor unions. If they continue to fight for an increase of official wages, they obtain new enemies – the workers themself. It depends on the power of the unions how important this hate factor becomes: If the contract obtained by the union is obligatory only for union members, the only result will be that network members leave the unions. If the union contract is obligatory for the whole firm or even whole branches (like in Germany), unions will have to survive the hate of non-members, who, with increasing official wages, have to pay more taxes and social security payments from the same wage (which is fixed in their real contract). It seems hard to expect that the unions will survive such a conflict.

On the other hand, if the unions participate in the network, they would have to learn to behave in a civilized way. And all the government support for them will be lost.

The loss of power of the labor unions will have positive effects on employment.

13.8. **Possible consequences of the decreasing tax base.** Will the state be able to survive an essential reduction of his tax income? This is questionable. A rational firm would be able, in a situation with reduced income, to get rid of all unnecessary or less useful parts, and leave only the really necessary parts. But the state is not a rational firm. The outcome is predictable – all the unnecessary bureaucrats preserve their jobs. The reduced income of the state will lead only to reduced wages for them.

Once this state has been reached, one can expect several consequences: First, once the state does not pay, one has to look for other income possibilities. One of them is corruption. Thus, the decreasing tax income leads to a further increase of corruption. Then, people will be less eager to work for the state. As bureaucrats, they are not famous for their eagerness anyway, so that means they will simply do nothing at all, and, instead, take a job at some real working place for real money paid inside the network. In the age of the internet, one can even force people to sit on their official working places, but they can nonetheless make other jobs during this time. To control what they really do would require even more bureaucrats to control them, but there are not enough money to pay them.

14. The Golden Rule

Up to now, we have not considered at all the very content of the rules.

There was a reason for this: It is, last but not least, left to the user of the network. So, the content may be very different. Nonetheless, I would like to make some suggestions for the content which I find important for the libertarian movement as a whole.

The primary suggestion is about the central, decisive role of the Golden Rule.

14.1. **The meaning of the Golden Rule in the network context.** The Golden Rule is a symmetry principle: You should forbid yourself everything you don't like if other people do it to you. So, after accepting the Golden Rule, you have only two choices in every case: Or you accept a general rule which forbids you to do it to somebody else. Or you allow everybody else to do it to you.

The usual formulations of the Golden Rule have been influenced by etatist thinking about general laws obligatory for everybody. So it seems necessary to clarify the meaning of the phrases like "to allow" or "to forbid" in the network context. The very point is that your rules are only restrictions for your own behaviour. Nobody else is obliged to follow your rules. So what does it mean "to forbid" or "to allow"?

The answer is quite simple: You have your rules for legitimate self-defense. The boundary of your right for legitimate self-defense is an important part of your rules. And the notion "to allow" has a simple and clear meaning: If you allow other people to do something, you have no right to use force against them in self-defense if they do it – you have allowed them to do it, so, doing it is not an attack and you cannot use self-defense as a justification for the use of force. If you, instead, forbid other people to do something, it means that it is, according to your rules, legitimate for you to apply, in self-defense, force against people who behave in this way.

So, in above cases, it is not the behaviour of others which is regulated, but, in full agreement with the general concept of the network, it is your own reaction on the behaviour of others which is specified by these notions.

14.2. **About the justification of the Golden Rule.** If humans would be completely equal, so that they would accept exactly the same rules, and if they would always hold all their promises, then the acceptance of the Golden Rule alone would guarantee a peaceful world. Of course, this is not our world. Human beings are, fortunately, different – everything else would be boring. But, as a consequence, they will never agree completely about their rules. Therefore conflict, even bloody conflict, remains possible – the unfortunate side of the differences between people.

So even if everybody follows the Golden Rule, our world would not be without conflict. But does this mean that the Golden Rule itself should be rejected? Certainly not. Those who do not accept the Golden Rule can be characterized as especially anti-social people. In fact, in their case conflict is not an unfortunate consequence of the differences between the people – conflict with them would also appear if all the other people were similar to them. Even if there would be no differences at all between people, and even if everybody would follow their own rules without a single exception, there would be conflicts between such sociopaths.

Therefore the acceptance of the Golden Rule allows to distinguish two very different groups of people. The first group can be named *aggressors* – they start conflicts with other people even if these follow the very same rules they accept as just for themself. The social order they prefer is one where other people have to accept their superiour position. All other people – those who accept the Golden Rule – may also appear in conflicts. But these conflicts are not caused by some inherent failure of these people, but by differences between different people. They are at least able to live in a peaceful way in a civilzed cociety. So we can name them *civilized*.

There is only a single unreasonable exception from this rule in traditional ethics: An exception for a single organization, the state. But, of course, it is reasonable to apply the Golden Rule to organizations too. An organization which does not accept the Golden Rule is also anti-social, aggressive, and dangerous.

14.3. **Comparison with the non-aggression principle.** Here it seems useful to compare the power of the Golden Rule with that of the non-aggression principle. The non-aggression principle regulates the application of force. But it does not and should not forbid every use of force. There is, last but not least, justified use of force, as in case of self-defense or defense of others. The question is what can you conclude if somebody accepts, in his rules, the non-aggression principle? It is almost nothing. Indeed, you have to look first at his rules defining the boundaries of self-defense. It may, for example, contain the idea that if you don't pay a regular tax to him you violate his rights and therefore he obtains the right to apply force against you. So, the meaning of the non-aggression principle may be easily and heavily distorted by a lot of details hidden in other rules.

In fact, if one defines the rules of self-defense in a way which violates the Golden Rule, allowing oneself to apply force under the label of self-defense in much more situations than one allows other to defend themself, we have a quite obvious distortion of the meaning of the non-aggression principle. An example would be a slave-owner, who considers an attempt of the slave to run away as an attack on his property which justifies self-defense of his property rights.

In other words, a meaningful interpretation of the non-aggression principle in fact presupposes the acceptance of the Golden Rule. Without the Golden Rule as a background, it is not more than a way to legitimate the own aggressions by naming

them self-defense or, correspondingly, the delegitimization of the self-defense of others by naming it aggression.

In this sense, the Golden Rule is more fundamental than the non-aggression principle. Of course, the Golden Rule, taken alone, is also weaker than the Golden Rule together with the non-aggression principle. But it has an independent value. One who rejects not only the Golden Rule together with the non-aggression principle, but even the Golden Rule taken alone, is obviously more dangerous, more anti-social than one who accepts the Golden Rule, but rejects only the non-aggression principle.

I think it is important to recognize this difference. In particular, it can be applied to the state. The state violates not only the non-aggression principle, together with the Golden Rule, but already violates the Golden Rule taken alone. This makes this organization even more dangerous and more anti-social. And, by the way, the non-aggression principle without the Golden Rule is not violated by the state: The Orwellian redefinition of aggression by the laws of the state, which classifies self-defense against taxation by the state as aggression and names aggression by the state "enforcement of laws", is, of course, indefensible – but only if one accepts the Golden Rule. Without the Golden Rule there is not much to object.

So, my argument is that the case against the state is much stronger if it is based on the Golden Rule, and not on the non-aggression principle.

The non-aggression principle has also other problems: It answers a simple yes-no question. You violate my property rights – I have the right to use force in self-defense. But in human relations we often have minor disagreements about property rights. Reasonable rules have to care about the possibility of escalation of such conflicts. The non-aggression principle does not care. So a reasonable set of rules may be in conflict with the non-aggression principle (or at least with some particular interpretations of it) if it does not allow, for example, to use force in self-defense if the property violation in question is not serious enough.

To use a principle which may reasonably be rejected by reasonable people as the foundation of libertarian ethics seems unreasonable to me.

If we base libertarian ethics, instead, on the Golden Rule, this gives also another advantage: There may be other people who disagree with the non-aggression principle, but accept the Golden Rule. To live with them may be more or less problematic, in dependence of their particular rules. If they, for example, use slightly different versions of property rights (for example, about apples falling from your trees into his garden) and reject the application of force in case of such minor violation, one could possibly live with them. But even if the conflicts are of more serious character, theses people seem much less dangerous than the state already because they accept the Golden Rule. In particular, in our conflict with the state they are our natural allies.

So if we base libertarian ethics on the Golden Rule, we have a much better chance to cooperate with them in our fight against the state.

14.4. **The ethical content of promises.** The Golden Rule can lead to a slightly paradoxical result. To explain it, let's introduce the notion of the ethical content of a promise: The ethical content of a promise is greater if the promise is more restrictive, if it is easier to establish if it has been broken, if the accepted penalty for breaking it is higher, and if there are more accepted arbiters who can decide if the promise has been broken. This notion is the ethical analogon of Popper's

notion of "empirical content" of a theory: In fact, it is simply the empirical content of the theory "X will hold his promise".

The notion of ethical content is a useful one if we want to establish the reputation of people depending on their promises. A higher ethical content of your promises gives you higher reputation. Now, the most important way of increasing the ethical content is to accept some additional promise: The ethical content of the promise "A and B" is higher than the ethical content of "A" taken alone.

The notion of ethical content does not allow to define a complete ordering of different sets of promises. There are many cases where it does not give an answer which of the two sets of promises has higher content. In fact, the cases where a unique answer can be gives are only exceptional. In the language of mathematics, such an ordering relation is named a "partial order". Nonetheless, it is useful, because in the rare cases where it gives a unique answer we can make unique decisions: Those who make promises with higher ethical content are preferable.

In fact, this applies even in the case where the promise defines a behaviour you don't like. Say, X tells you "I come tomorrow to kill you." This allows you to prepare yourself, say, to buy a gun, or to run away. You may feel uncomfortable that night, but the situation is much better in comparison with the situation where he comes tomorrow to kill you without telling you about this before. In fact, compare this with a slightly different situation, where you ask a friend what he thinks X will do. If your friend tells you that X will certainly come tomorrow to kill you, and it happens that X really tries, but you survive because you have been prepared, you will thank your friend very much. But the prediction about the future behaviour is the same. So, even in this extremal case the general rule that higher ethical content of a promise is preferable holds.

14.5. **General rules vs. additional promises.** So, the general situation is that if I give another promise, A and B instead of A only, this is something preferable for you.

But now assume I have accepted the Golden Rule. Now, say, I have also accepted several rules, say, A, B, and C. What follows from the Golden Rule about these rules? I have to allow others to behave in ways which do not violate nor A, nor B, nor C. That means, if I add yet another rule D, I have to allow less: It is allowed now to behave in ways which do not violate nor A, nor B, nor C, nor D. Behaviour which violates nor A, nor B, nor C, but violates D is no longer allowed. That means, if you behave in such a way, I'm allowed now to apply self-defense against you.

In other words, if I accept the additional rule D for myself, I also reject the rule which forbids me to use force if you violate D. So, accepting yet another rule no longer increases the ethical content of my promises. A behaviour everybody likes to see – that I accept additional restrictions for myself – now becomes questionable, because, on the other hand, I also give up some other restrictions.

In particular, an asket is no longer a person which deserves high reputation because he is able to follow extremely restrictive rules, but becomes dangerous to people who are unable or unwilling to follow similar restrictive rules. There are, of course, such fanatical askets who have the aim to force everybody to follow their particular asketic rules. But there are also socially acceptable askets, people who do not want to force others to do things they don't like, people who deserve high reputation.

The Golden Rule as defined up to now does not allow to distinguish these two types of askets. So everybody will qualify the socially acceptable asket as at least potentially dangerous. But what to do in this case? A simple but reasonable way to solve this problem is to introduce a subdivision of our rules into general rules and particular, additional promises. Then, the Golden Rule has to be applied only to the general rules.

In this case, the socially acceptable asket accepts A, B and C as his general rules, allowing others to behave as if they would accept A, B, and C. Instead, the special asketic rule D he can classify now as a particular, additional promise. In this case, we are allowed to behave as if we would accept only A, B, and C, as before. So, accepting the promise D is, again, a pure increase of the ethical content of the askets rules.

Instead, a modification of the general rules, defined as those rules the Golden Rule has to be applied to, is nor an increase, nor a decrease of the ethical content: Every modification in the restrictions I accept for myself leads to a similar modification of what I allow others, but in the reverse direction.

14.6. **The preference for tolerance.** What should be the character of the general rules? This seems to be a complicate question. But, given that people are different and therefore may like to do things that you don't want to do, those with less restrictive general rules seem to be preferable partners – it is more probable that they tolerate your own strange habits and interests.

The aggressive asket can be, instead, identified by classifying very specific, very detailed rules, which prescribe almost everything in detail, not as additional private promises but as part of his general rules. That means, whoever does not follow his very detailed "general rules" has to be afraid of him.

The preference for tolerance is purely rational. The rules of the aggressive asket have a lower ethical content than the rules of the tolerant asket. So it is rational for everybody to prefer the tolerant asket.

But it is not only the comparison with the tolerant asket. Let's compare simply different sets of general rules, assuming that there are no private rules. Now, assume the difference between X and Y is that Y accepts an additional general rule A. Without the Golden Rule, the ethical content of Y's rules would be higher. With the Golden Rule, we have no longer a unique preference. On the one hand, Y is now not allowed to do A. On the other hand, X allows others to do A. What is more important now?

Usually people care more about their own freedom. So, usually Z would prefer rules where he is allowed to do A, and care less about the minor problem that X is also allowed to do A too. So Z will prefer to cooperate with X.

There are, of course, exceptions. The exception is that Z considers X doing A as dangerous for himself, and the danger as greater than his own interest in doing A. In this case, Z will accept the rule forbidding A too, and will prefer to cooperate with Y.

These two typical cases lead to a simple resulting rule: In your general rules, you should forbid yourself only things which are *really dangerous* to other people.

I have used here "really dangerous", not simply "dangerous", for the following reason: A little danger will not be sufficient. People prefer their own freedom of choice. So the fear of others doing X should be large enough to be stronger than the own interest to do X. Of course, to estimate the meaning of this "large enough"

has to be left to the participants themself. In particular cases, science can support the decision-making by giving scientific results about the dangerousness of certain behaviour for other people. A general consideration as given here cannot.

So the classical difference between law of a liberal state and morals, where laws are justified only to forbid behaviour which is really dangerous to others, while moral rules may be much more restrictive, appears in the network in a natural way: The laws of the state become the general rules, the rules connected with the Golden Rule. The morals become the additional private promises. The rational rule to distinguish the two remains the same: The general rules should forbid only really dangerous behaviour.

14.7. **Property claims.** If one considers the Golden Rule formally as a rule which forbids any legal monopoly, which requires me to allow everybody else what I'm allowed to do myself, property seems to be forbidden: It is a legal monopoly right. I have the right to do with my property whatever I like, and nobody else has this right without my explicit agreement.

This may be a problem for libertarian philosophers who would like to use the Golden Rule as some absolute ethical rule. But from point of view of rational ethics such a problem does not appear. It is simply irrational for human beings to accept a rule, however named, if it forbids property. So, particular property claims are another thing which has to be considered outside the scope of the Golden Rule. The Golden Rule is, therefore, a metarule applicable to general rules. It should not be applied nor to additional promises, nor to property claims.

As the additional promises, as the particular property claims are, therefore, possibilities to modify the Golden Rule, to apply it to a society of different people.

Promises and property claims have a different sign: Additional promises increase the ethical content of the own rules, property claims decrease it. This is in full agreement with the rational notion of ethical content: We prefer people which make less property claims, because they are less likely to be in conflict with our own property claims and gives us more possibilities – for example, to take something which he does not claim as his property.

I have intentionally named the claims discussed here as property claims, not as property rights. It is not the job of the network to solve conflicts between different people, but to inform people about what other people accept as just. The main purpose of such information is the prevention of conflicts, not their solution. If the network allows, in an easy way, to find out if a car I want to buy is claimed as property not only by the seller, but also by somebody else, this is useful information for me. By not buying it I can possibly avoid a conflict.

14.8. **Justification of property claims.** This situation is not nice for the seller of the car. Many people will not buy the car at all, other only for a large discount. This may be a motivation to solve the property conflict: The mere existence of the property conflict decreases the value of the property, at least on the market.

The problem with this is that somebody could, just because he hates somebody else, claim all his property. Without the intention to really take the property away, but simply to decrease their market value for the owner. How to prevent this?

The best idea seems to be a formalism for the justification of the property right. There will be simply some standard forms of property claims. I buy something, the previous owner signs that I have paid. The record of this, with the date, will

be stored. You create something, say a picture, and leave a note that you have created the picture, with date and photography, and own it. A fabric produces a device which, in the age of chips everywhere, has a chip with an identification number in it, and the corresponding record with the identification number, the date of production, and the ownership claim for the owner of the fabric is submitted into the network.

Of course, there will be problematic cases. I have received something from you in exchange of some service, claim to have done everything, you disagree and claim your property back. It seems, the reasonable way to handle this is to have some record for the fact that you have given the thing to me, but no record of the final transfer, instead another record about your claim (with justification) and my refusal to return it (with justification).

This would, in this case, not solve the conflict. But it would allow other people to differentiate between completely unjustified claims and claims which have at least some base.

In a world full of states who like to extort the property of people it would be dangerous to give such detailed information about actual and previous owners. But the network would, in such an environment, have to care anyway about the security of the participants. One way would be to support pseudonymous accounts. Such pseudonymous accounts could be used to manage your property claims without informing the tax inspector about your property.

15. The state as part of the network

We have already noted that the network can start to work already in a world controlled by states.

And we have also considered in section 12 the possibilities of defense of the network against attacks by the state. And we have considered in section 13.1 what happens if the network is legal. Here we continue this consideration: We consider the case where the network is not only legal, but the state itself participates.

15.1. **Participation of states and other criminal organizations.** We have introduced now two types of exceptions of the Golden Rule: addtional private promises and property claims. We want to introduce here a third class. It consists of general rules with an exception for yourself. These are, therefore, simply exceptions from the Golden Rule.

What is the purpose of introducing this type of exceptions? The point is to allow states and other criminal organizations to participate in the network in a more natural way. It is simply the way they usually formulate their rules – as general laws which are obligatory for everybody else except the state itself. So, in this form the laws of the states and the general rules of the individuals become comparable in a much more natural form: The civilized individual, who accepts the Golden Rule, uses a general rule, acknowledging that this rule is binding for himself and that he has to tolerate behaviour of others in agreement with the rule. The criminal organization, instead, accepts possibly the same general rule as a law. This means, as well, that it promises to tolerate behaviour of others in agreement with the rule. The difference is only that the criminal organization does not accept the law as binding himself.

This difference is certainly important, but, on the other hand, there are many situations where I do not care about the difference, but where I simply want to

know if a certain type of behaviour is unproblematic in a certain area or not. In this case, I have to look for what the relevant actors in that region tolerate. In such a situation I do not care too much about the exceptions these criminal organizations make for themself.

It is worth to recognize here that, in a world where states and other criminal organizations exist, it would be certainly preferable to have them participating in the network too. It makes it easier to get information about their laws and their reputation for holding them, and it will lead, in a natural way, to a competition between the states. Other criminal organizations may participate in this competition too. Non-state criminal organizations are not necessarily worse than states. For example, a separatist movement may want a separate state (and has, therefore, to be qualified as criminal) but a much more libertarian one, a minimal state. One has to recognize in this context that the network will be very helpful for more civilized (say, separatist) organizations, but less helpful for the more dangerous totalitarian organizations. In any way, they can use the network to establish a reputation for having civilized rules and for following their own rules.

The competition between states and other criminal organizations for reputation in the network would follow the same rules as the competition between civilized citizens and between members of above groups. Rule breakers will be despised and loose potential cooperators. And rules of different persons may be compared, first of all by their ethical content.

Of course, every exception from the Golden Rule – the difference we name here "criminal" – decreases the ethical content of the rules of the given organization. So, the state has no chance to compete in the domain of ethical content with a civilized citizen. This fact, taken alone, becomes much more obvious if everybody – citizens as well as criminal gangs – participate in the network.

There are other advantages of the competition. For civilized people it is obvious and clear that they would have to accept independent arbiters. States and other criminal organizations are not used to allow independent arbitrage.[2] In a fight for reputation, this may change.[3]

The real point is that this competition may be the tool to transform the current state into a more civilized organization.

15.2. **Making the state predictable at all.** In a purely formal way, the state is predictable today. All what the bureaucrats do is prescribed by some written laws. The problem is that there are so many laws that it is impossible to know them all, which effectively makes the state unpredictable.

This remains extremely problematic if the state decides to participate in the network. Simply to put the own laws, article by article, into the network is, of course, possible. And even this gives some advantages. Having all laws in electronic form in the network, one can use at least search programs to try to find something relevant. But one of the advantages of the network is one can use programs to

[2]I have to admit that I don't know enough about criminal organizations here. It is reasonable to think that what is presented in the etatist media as a unique organization like "the mafia" may be a group of sufficiently independent small criminal enterprises which solve their conflicts by arbitrage, where the "bosses" are, in fact, more close to arbiters.

[3]For example, the US libertarian movement could fight for the right of state courts to make final decisions about constitutionality of federal laws.

compare the rules of different participants. Here, states cannot compete, at least in their current state.

So, the existing laws of states are simply not compatible with the network, in particular with the software used in the network to compare the reasonableness of the rules accepted by other people. Moreover, the very idea to let the state participate in the network is not an idea which would be acceptable for the established political parties. Probable such a decision is possible only after a quite serious change of the political power. A possible scenario would be the development of political parties as organization in the network who propose completely new sets of laws for the state, new sets which are compatible with the standards developed in the network, as discussed in section 7.

Therefore the reform would have to be a quite radical one, with a political fight for support inside the network. So, the great number of laws of existing states would not be a really big problem at all – the new law would be developed by political parties in the network from the scratch, in agreement with the established network standards and therefore testable and regularly tested with the standard test software applicable for usual human beings.

Of course, it does not follow that the resulting new law are very much better than the old ones. They can, at least partially, even become worse. Nonetheless, what would happen would be a quite radical transformation – almost all existing laws would have been replaced by new ones. So a lot of unnecessary regulation would disappear overnight, not after some long political fight between lobbyists who defend these laws and the rest of the world, but simply because these regulations have not been part of the program of the new network-based parties.

If the state starts to participate in the network, this is a large step forward in the long way toward the transformation of the state into a civilized society. The first step, the step which makes participation itself meaningful, may be the most problematic one. In fact, one needs a lot of legal reform to make the state, even in the complete form as today, with police, jail, and taxes, compatible with the standards of the network.

15.3. **Transforming the state into a civilized organization.** So assume the state is in the network. Its laws remain monopolistic laws of a state, violating the Golden Rule, instead of rules of a civilized organization. Nonetheless, they are compatible now with the accepted standards for rules as used in the network. So people can compare now the laws of different states using the same software, and behind that the same general principles, they use for the evaluation of other organizations and persons.

Its remaining violations of the Golden Rule puts the state into one category with other criminal organizations, as organizations which violate the Golden Rule.[4]

Now, the software used to evaluate the rules of other people automatically recognizes every removal of a legal monopoly of the state as an advantage – it gives additional freedom to yourself (to compete with the government in this domain) and makes the government itself less dangerous for you (it will not start violence

[4]Here, the oganizations considered today as criminal will heavily object – most of them respect the Golden Rule, and they are named "criminal" today by the state only because they provide illegal services to customers like illegal drugs and so on. So, I don't have in mind such providers of simply illegal services. I name an organization "criminal" if and only if it rejects the Golden Rule.

if you start competition). Of course, some people, believing into etatist ideology, may prefer some other software, which prefers aggression by the state against competitors in some domains. And there will be, of course, such special software for evaluating states based on other principles. But the very fact that one needs special software to present states in a better light, instead of using the same principles for all, so that states appear as criminal organizations, is a good argument against the state.

15.4. **A program for a libertarian party.** It is hard to say if there is a possibility of a peaceful transformation of the state into a civilized organization. Historical evidence is not in favour of such a hypothesis – the typical evolution is in direction of increasing government power. But there are exceptions, in particular the liberalization in the communist states after Stalin's death and the final collapse of communism.

But the situation we have in the situation described here is a completely new one. First, we can assume a quite strong libertarian ideology in the network. Then, the state itself is already weakened in some very essential points: It has no longer the possibility to control the real income of the people, which destroys its tax base. So the tax revenue has been, probably, already heavily reduced. Then, it has no longer the ability to prevent freedom of contract, and in civil law its power is gone.

Moreover, political parties have to put their proposals for legal reform into the network, for evaluation by the network software.

In this situation, a lot of things may change. In particular, there will be a simple program for a libertarian party. It fixes the decisions of its members of legislation in the following way:

(1) Proposals which improve the ethical content of the laws of the state have to be supported.
(2) Proposals which don't improve the ethical content of the laws cannot be supported. The only exception are modifications which can be split into two parts:
    (a) a part which improves the ethical content and, in particular, decreases the criminal character of the laws (that means, removes some violations of the Golden Rule) and
    (b) a remaining modification of rules such that the modified rules themself are compatible with civilized behaviour (say, increasing prices for some services provided by the government on a free market).
(3) Proposals which decrease the ethical content of the laws of the state have to be rejected;
(4) Proposals which add or extend any new violations of the Golden Rule have to be rejected;
(5) For all other proposals, or neutrality or rejection is allowed.

And, of course, it makes an own proposal for a new law which is a completely civilized one.

In fact, making exceptions from the second rule is dangerous, but there seem to be reasonable situations where not to support such things would be stupid. Imagine a transformation of a legal monopoly into a free market service where the government service is no longer supported by tax money, so that taxes may be decreased. But, as a consequence, the former monopolistic service, now a completely

civilized participant of the market, obtains the right to increase its prices, which was previously fixed by law. This would be a completely libertarian reform, but would remove the restriction of the fixed price from the service and in this way decrease the ethical content a little bit.

The danger of misuse of such exception clauses is a serious one, so it has to be severely restricted. Those who will be elected, of course, have to promise to follow these rules in the network. So, to elect this party would be a safe bet for libertarians, independent of their political preferences and interests. And for those who use the standard software, without special handling for the state, for evaluating party programs, this party will be clearly the preferred choice.

15.5. **Strategies for improvement of the state.** An interesting question is which part of existing laws could be preserved, with some modifications, in a civilized society.

The laws which regulate the behaviour of state courts are usually almost completely civilized laws – the state is the owner of the court rooms and can decide about the ways state courts work. The only laws which have to be removed are laws which force citizens to cooperate with them, say, to tell there anything at all. As far as they regulate only state courts, they are civilized. Any arbiter in the network also has rules for his own behaviour.

In a similar way, laws which regulate industries which are completely owned by the state may be easily transformed into civilized rules: All what has to be removed is the legal monopoly. Everything else, then, has to be reinterpreted as regulating the rules of behaviour on government property.

Note that this simple modification is much easier than the usual way of "privatization" of various state-owned industries – usually a large body of unnecessary regulations. If the government monopoly is removed, this is all we need. If the former government monopoly is a natural monopoly – so what?

Then there is a great complex of laws which have to be only slightly modified to become compatible with the Golden Rule – all the laws which are justified today with the label of "consumer protection". They can be easily transformed into laws which, instead of forbidding something, simply regulate the use of a label named "approved by the government of X". In fact, every person or organization X owns its name and, therefore, has the right to decide about the conditions of using a label "approved by X", and the government is no exception here. The resulting legislation about the use of this label, however stupid, complex, or otherwise unreasonable, would be completely civilized, in full agreement with the Golden Rule, and therefore completely unproblematic. But almost everything regulated today can be replaced by regulation relevant only for those who want to use the label "approved by government".

The subtle point here is, of course, that only the official, claimed aim (the protection of the public) will be reached – the consumer will be informed about what the government thinks about the security of the things. But the hidden, illegitimate intention of the lobbyists for this type of legislation – to preserve established firms from competition – is no longer reached. So, the lobbyists would protest heavily.

But to justify more, one should argue that poor stupid consumers have to be prevented from using products not approved by the government even in a situation where they know that the product is not approved by the government. Such paternalistic argumentation is, of course, sometimes used. But members of the network

will be unable to follow such arguments. States which do not restrict themself to labeling, but forbid to sell non-approved things, will be disfavoured. The reason is not so much that they don't like paternalism – even if this is quite probable. The reason is simply that their programs for evaluation of the rules of people would fail to evaluate the state as predictable at all, given the large amount of things which are forbidden.

15.6. **Other transformations of state laws.** The so-called "consumer protection" is, of course, not everything which makes the state unpredictable. There are a lot of laws which can be modified in such ways that their content becomes more compatible with the rules of the network. In particular, there are a lot of laws which are in fact only relevant for small minorities of people, usually potential and actual competitors of the lobbyists who have supported the law. But, of course, who knows without reading them? It happens that somewhere, hidden in some law which seems completely irrelevant to almost everybody, appears to be some law whose appropriate place would have been the penal code.

So even if one would not like to reject such laws completely (the best thing which one can do with state laws in general), one could make them more compatible with the network by placing some restrictions into the initial part of the laws which states: 1.) that the law is relevant for a certain, well-defined group of people, and 2.) that the maximal penalty for violating this law is equal to a certain maximal penalty. With such restrictions, the law could possibly be identified as irrelevant for many people even if the program is unable to identify its content.

There are other laws which become worthless for the networkers almost automatically: Whatever is decided by civil courts becomes irrelevant once the participants don't use state courts anyway to resolve their conflicts about contracts. The large amount of restrictions of freedom of contract becomes de facto irrelevant in the same way.

15.7. **Transformation into a stateless society.** Is it possible, at least in principle, that such a transformation ends in a really stateless society?

It seems, at least, not impossible.

The network itself already destroys government monopoly in one of the few domains where minimal state supporters have seen a necessity for the state – arbitrage and enforcement of contracts.

There are a lot of questions I have not considered here, in particular that of production of defense, and the problem of conflict resolution in cases where no contractual obligations exist between the conflicting parties. But it should be noted that the worst thing related with national defense – the slavery named obligatory military service – is decreasing all over the world. The armies all over the world become professional, and in this sense unproblematic.

On another level, private security firms also play an increasing role all over the world, with gated communities becoming more distributed. There is the moral objection that they are only affordable for the rich, but I assume the reader is sufficiently libertarian to reject this objection himself. From point of view of a libertarian movement, this may be even an advantage: First, the rich and powerful solve their own security problems in a civilized, private way. Once they start to prefer such private services as more reliable than state police, they will tend to lobby

for a removal of legal restrictions for these private agencies, so that they can take over more and more functions of governement police in their gated communities.

Given that the rich and powerful solve their security problems in a private way, they have no private motivation to give government police any power. Government police becomes police for the poor, and, correspondingly, ignored. The expected decrease in tax support for the state in general will lead to decreasing financial support for the police too. At some point, the poor will also create their own private security agencies, as well as their private gated communities. Given the nonsensical minimal wage laws, there is a sufficient number of jobless young men to do such jobs for cheap, thus, affordable also for the poor. In fact, similar things are already happening in many slums of the world. With detoriating police power, this simply becomes a necessity.

So, the problem of government police may disappear itself, in a quite civilized way, with the increasing role of private security services and decreasing tax income of the state.

16. Conclusions

With modern information technology, it is possible to manage a network society where everybody defines his own set of rules – rules he accepts as just and obligatory for himself – together with just penalties for breaking these rules and fair arbiters. Those who do not accept their penalties after violating their own rules will be punished by an entry in an open black list – a sufficiently strong penalty in a large network.

Some minimal standardization is necessary for this, but the resulting restictions of the freedom of choice of the own rules are quite unimportant. The evaluation of the rules of other people can be managed by sufficiently simple software. The network allows also automatic procedures for the establishment of reputation.

All software programs for the evaluation of other people depend on parameters which can be controlled by the users of these programs. Despite the large number of such parameters, the possibility to use the parameters preferred by other trusted persons as a starting point makes the use of such programs sufficiently easy for newcomers.

Only a few proposals have been made about the content of the rules. The Golden Rule has been considered in some detail. In such ethical considerations only rational, utilitarian ethics (educated self-interest) has been assumed. Because in the network everybody is evaluated by everybody else in dependence of his rules and his reputation to follow them, the necessity to find cooperators in the network is sufficient to enforce reasonable rules.

Defense against possible aggression from states is possible, various methods have been considered. One important prerequisite is the possibility to use the network pseudonymously and to control each bit of personal information one gives. The main problem with pseudonyms is that it is much harder to evaluate reputation automatically: One has to be able to distinguish fake subnetworks created by a single person from networks of real persons. Nonetheless, some sufficiently safe possibilities for the management of personal information have been presented which allow to solve this problem.

Various other questions have been considered, in particular the influence of the network and in particular of the freedom of speech in the network on the ideologies of

network participants. Especially interesting are various economic consequences like an effective increase in the freedom of contract and freedom of arbitrage, increasing possibilities of tax evasion, of a network-internal banking system, improvements for illegal markets and a shadow economy in general.

The state will be weakened in several ways: Loss of control over income paid in the network-internal banking system, loss of control over private contracts and their arbitrage, decreasing tax income because of increasing shadow economy, increasing corruption. Remarkably, it is argued that the network is especially attractive to the rich and powerful. This further weakens the support for the state, making the libertarian revolution attractive for the ruling class, and, so, hopefully as peaceful as the anti-communist revolutions.

The main point is that the network can be created already in a statist environment, and gives a lot of additional freedom and various other advantages to participants already in such an environment. Libertarian solutions for many problems may be worked out and developed, a libertarian informational and organizational infrastructure developed.

So, this is a proposal which we can start to realize now. Moreover, it is not related with large costs: To start the network, only appropriate software has to be developed. A few simple applications, like secure file-sharing, will allow to attract sufficiently large numbers of users.

So we don't have to wait for the collapse of the state. We can start to act now.

References

[1] Hans-Hermann Hoppe, The private production of defense, mises.org

[2] Hans-Hermann Hoppe (ed.), The myth of national defense: Essays on the theory and history of security production, Ludwig von Mises Institute,mises.org