"The in secrecy negotiated TISA trade agreement has a direct impact on our privacy, it threatens the protection of network neutrality and could further reduce the security levels of software. In the event of the USA pushing through some crucial points, there is a threat of a lowering of our privacy levels and even more spam. In TiSA trade is placed above fundamental rights. So an intense public debate is necessary in order for industry lobbyists not to take the lead."

Summary critical points network policy
Freedom of trade before data protection

[Annex Electronic Commerce, Article 2, 4]
[Core Text Article I-9]

Participants may have their privacy rules but: The regulations of individual states may not constitute "unjustifiable discrimination" or "trade barriers". No one is allowed to restrict a service provider to transfer, access, process or store data within and outside a participant's territory.

EU has not yet positioned itself about data protection. With TiSA, the EU Basic Data Protection Directive would be more or less ineffective if it disadvantaged other participants. The demand for an "appropriate level of protection" for third countries to which data is transferred is eroded. A "race to the bottom" is to be feared, with all of them following the lowest common denominator.

For example, if a provider from a participating country with weak data protection rules offers services to EU citizens, the EU can not impose any kind of data protection clause on them because they can always be interpreted as barriers to trade. In the third country, no effective controls can be carried out, whether conditions are respected and also where the data is passed on to. In the US, for example, there is no uniform, stringent data

protection legislation, but only sector-specific regulations.

For example, the purpose-setting is called into question, which in many countries outside the EU is weaker or not at all anchored in the right to privacy. WhatsApp came into criticism, when in September it began to pass all numbers from the telephone books of users to Facebook. This does not correspond to the original purpose of the service and includes, in particular, data from those who do not even use WhatsApp and can not agree to or disagree with the transfer. The control over what data of citizens from foreign countries is passed on to which companies and other states is practically impossible.

No obligations about the location of the companies

[Annex Electronic Commerce, Article 8]

Nobody is allowed to demand that providers are located in their own territory. And also not to store the data on their own territory. Therefor the jurisdiction of the location country is applied. This is on the one hand a problem for data protection regulations, but also for the possibility of users / consumers to appeal (someone from the EU would have to then complain in the USA, for example).

In addition, there are problems with the access to data by law enforcement agencies and intelligence services. This is to say: If the data is stored in the US, it is also given to the authorities there.

Examples: Max Schrems has appealed against Facebook in Ireland. If a company is now without a seat in Europe, it is a problem for EU citizens who want to assert their rights. Even if Europeans with Juducial Redress Act can in principle complain about data breaches in the USA, the way is even more complicated than in Europe. First the administrative route has to be tried, then one can turn

to the courts. There are also generous exceptions: if companies were to be restricted to give data to law enforcement authorities, one can not take action against it. Likewise when national security interests are concerned.

The article also limits companies employing e.g. Cloud services in the EU, from position themselves more positively in the market because of a better data protection, since US companies can not be discriminated against.

Exception for national security

[Annex Electronic Commerce, Article 13]

Nothing in the chapter on electronic commerce applies to the protection of "essential security interests" of participants. What is meant by these security interests is not defined. This could be a huge exception for law enforcement, intelligence services and Co to do all sorts of things.

The US government can simply query user data from companies. If European user data is now available in the US, it becomes even easier for US authorities to get this data.

Network neutrality

[Annex Electronic Commerce, Article 7]

As with data protection, network neutrality must not be a trade barrier. "Reasonable" network management has to be allowed to be carried out. This is quite a rubbery term and allows the vendor in principle, to also pass through as reasonable so-called special services (passing lanes in the net). It is especially striking that the US is opposed to the EU's proposal to take the word "non

discriminatory" as a prerequisite for network management. This shows quite clearly that there is no interest in real net neutrality.

Intransparency of source code

[Annex Electronic Commerce, Article 6]

TiSA contains rules according to which no participant can require providers to disclose source codes. The exceptions for critical infrastructures contained in previous drafts do not apply, so even with software in nuclear power plants no one is allowed to check whether all safety conditions are met.

This is also a problem for software of routers and Co. Here it is particularly important that the security of software can be checked. Also in terms of the presence of loopholes und Co. A large portion of hardware comes from the US. So if, for example, the NSA is installing backdoors in routers that are coming to the European market, there is no way to check and prevent this. The same applies to security gaps. You'd have to blindly trust that the software is safe. Particularly in the case of critical infrastructures, such as control software for power plants or other control systems, it is unacceptable that one can not check whether the software satisfies the national safety requirements.

Unsolicited advertising

[Annex Electronic Commerce, Article 5]

States want opt-out and opt-in solutions for unsolicited advertising (aka spam). The US and others note that minimizing unsolicited advertising should be sufficient. The EU does not want that. If the EU is successful, the article is quite reasonable or harmless.

When companies send out advertising emails, one must

have the option to get out of the advertising distribution or have to agree to receive these messages in the first place. If the proposal of minimization is implemented, it is only necessary to send advertising messages as little as possible. There is no yardstick for this, the meaning of the article would be undermined.

Interactive Computer Services

[Annex Electronic Commerce, Article X.X]

New chapter, introduced by USA. Interactive computer services are defined so that everything is covered where several users access one server. Problem: The operators and users should be able to block and delete more or less arbitrary "and objectionable" content - as long as they have not created it themselves - without having to justify themselves and to be held liable. This is a free pass for the privatization of censorship, for example on the subject of nudity on Facebook.

[Exception for copyright violations, but that is not surprising]

Relevant formulation:

X.X 3. No Party shall impose liability on a supplier or user of an interactive computer service on account of:

(a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable.