

# Legal Challenges of Providing Global Online Services

Leena Kuusniemi

<b>1</b>	<b>Introduction</b> .....	288
<b>2</b>	<b>Terms and Conditions for Global Online Services</b> .....	289
<b>3</b>	<b>On Governmental Authority and Sovereignty</b> .....	292
<b>4</b>	<b>Babel – Language Requirements for Services</b> .....	294
<b>5</b>	<b>Legal Competence and Age Limits for Services and Content</b> .....	295
<b>6</b>	<b>Licenses and Separate Permissions to Seller Entity/Service Provider</b> .....	296
<b>7</b>	<b>King Content</b> .....	297
<b>8</b>	<b>Navigare Necessare Est – Navigation and Maps</b> .....	298
<b>9</b>	<b>Conflicts at EU-Level Legislation</b> .....	299
<b>10</b>	<b>Conclusion</b> .....	300

## 1 Introduction

This article intends to describe in a very subjective way some of the challenges I have personally faced when providing legal support for Services business unit in Nokia Corporation. I would be happy to offer answers, but I'm afraid that this article ended up being a list of questions. In no way underestimating the readers I must emphasize that I have been written solely on my own experiences spiced heavily with my own personal opinions, and have actually not even bothered to ask any of my colleagues to read this thru to find out, if they share my views totally or in some cases not at all. This is not therefore an article from or by Nokia Corporation or Nokia Legal, but written by Leena Kuusniemi, who has been lucky to work with very interesting dilemmas related to offering online services in almost every single country on this lovely globe we call Earth.

Reading different publications from government bodies, multinational organisations and interest groups it seems that providing online services for the entire world is the most desirable goal.

Most of such communicatees consist of sincere wish to remove obstacles of cross-border activities, facilitate operations and therefore providing the consumer widest possible choice of services.

Utopian view: a world where consumers will have open access to all services (including the Internet) any time and any place and service providers have fair and non-discriminatory access to delivery networks and customers. The offering would be shaped according to consumers' wishes and creativity, as online service could offer a truly unique way for the people to connect with other people or issues they are interested in and that they care for. Also, consumers would have easy and full understanding of rules that apply to those services, and choice of effective remedies if some service providers would choose not to respect rules and their customers.

Unfortunately the reality is far from this utopia: the rules and regulations are not only fragmented within any geographical area consisting of several countries, but also in conflict inside a one single country.

My intention is to describe the real experiences of an inhouse legal counsel working for an international company offering both hardware (devices and accessories) and software (services and applications) in almost every country in the world, "both" meaning that hardware and software are offered in combination, either free-of-charge or against a fee.

My personal firm opinion is that due to this fragmentation the world today is sadly open to only two kinds of players: either very small ones operating in a single country or perhaps market – or very large ones having capacity and resources to map possible risks, and sufficient muscle to discuss with authorities over unclear obligations and their possible interpretations.

One clear example effectively blocking any other than giant companies is the legacy intellectual property governing system aspects, such as territoriality and ad hoc licensing, meaning again that only those industry players with huge resources can even dream of clearing all necessary rights to offer music or other similarly protected works across boundaries. A small or middle-size company with adequate skills to purchase those rights might just simply not possess the

required negotiation power but must be satisfied with catalogue pricing and standard terms for usage.

This means that growing from a small start-up phase is near impossible, and this leads that there is not that much actual choice for the individual consumer. In order to offer wide choice of services, the harmonization or at least simplification of current jungle of laws and regulations is an essential condition. Otherwise there will be very limited amount of players: those having resources to analyse and take risks, and those who simply don't care.

## 2 Terms and Conditions for Global Online Services

The millions of people, who visit web-sites on daily basis, do not typically pay much attention to the links at the bottom of the web-page saying "Terms" or "Legal" or "Site terms", "Privacy Policy".

Not many more get excited when pushing the "I Agree/Accept" button when actually presented those Terms&Conditions, as a requirement to proceed to the services offered on a service provider's web-site or other source.

In this aspect the behavior does not differ that much from any other business transactions, one gets interested in terms&conditions only at the stage when something does not perform as was reasonably expected.

There are some very fundamental legal questions related to online service rules, the first being this: How is a binding legal agreement concluded between service provider and customer? And where?

I want to make a provocative example, which I have used often in connection with this topic:

If Drottningsgatan in Stockholm would operate as an online store, every single customer would have to prove they are of full age and sign an agreement at the door, accepting that the items visible are subject to possible specific legislation and restrictions or requirements, and that they need to pay for them prior to exiting (if they want to avoid committing a crime) and that they should not disturb other customers by shouting insults or harassing them in any way. Every customer would also be inspected on departure.

I have serious doubts that this would make those shops very popular and that people would be patient with such requests. To be blunt, this kind of operations would kill the business. One can argue that there are laws and regulations covering all that, so there is no need to declare the contents of law for every single person entering the store. It is reasonably expected that every single citizen knows the rules of commerce – even minors, who with ready money can buy whatever is offered in real world stores, with some minor exceptions such as harmful substances like alcohol and cigarettes in some countries.

For online services, do we need a specific agreement text that is approved by the customer i.e. end-user, or can either one refer to applicable laws only?

It seems that uncertainty has created unspoken demand of having explicit agreements with end-users in addition to any applicable laws and regulations. I also have some personal views that it is partly Anglo-American legal tradition that has leaned more towards agreements as a source for protection than law providing sufficient rules.

In early days of internet specific terms and conditions were certainly seen as advisable precaution to protect against unreasonable accusations of customers, who were often typically some kind of internet pioneers.

The next excuse was that in addition to the nerds the grand-mothers started shopping and it was advisable to underline certain processes to customers, as circumstances and general scenario differed from the usual set-up of “real” world.

But post-order shopping had been thriving for years, so it was reasonable to question this approach. If shopping online actually just means placing non-paper order for goods and services, why do you need 12 pages of additional terms and conditions. In addition those terms are very often in conflict with mandatory local legislation, for example in case where US- based company offers services to Europeans, who are entitled to have protection of their residence country’s customer legislation at nearly all times.

The discussion was not very lively due to a very simple reason: there was plenty of room for terms&conditions online. And using a very banal reasoning, it did not cost too much to secure the extra protection of getting specific agreement in place with a customer and store that for future reference.

The situation changes, when the screen is smaller than in your standard PC, such as is used in many mobile devices. Pushing pages and pages for the end-user to scroll down before acceptance is not a very end-user friendly approach so this puts the lawyers to work and also to question, what is really needed and why.

The challenge for example for Nokia services was the mere width and variance of them: music, maps, mail, storage for content sharing, games, and 3rd party services.

When looking at some service providers web-sites I found easily more than 20 different sets of end-user terms and conditions, in certain cases closer to 40 sets of terms and conditions. Quick calculation with translations for some 80+ languages meant easily 1600 variations of those terms and conditions. Any change or update would mean changes into all those language variants as well, causing loss of time and money, and perhaps end-users treated differently depending on their language area. Such situation would arise, if the change would not be implemented simultaneously due e.g. delays in the translation and validation processes.

Clearly there should be a more simple way to govern end-user terms, but first one should tackle the basic question of why a specific acceptance from the end-user was needed.

If there is mandatory legal requirement or protection for the end-user, one cannot override that legislation by an agreement. Only in case that law allows for deviation, does the agreement on that deviation make any difference.

The real dilemma is rising from the fact that law is silent in many cases, but lulling oneself into illusion that informing the end-user by terms&conditions gives security, is not recommendable. The guidance for the end-user on service features and other conditions is clearly given more effectively somewhere else than in the legal text, for example in good and transparent marketing and offering guidance and tutoring for the end-user.

In my personal opinion such clear information also reduces substantially any legal risk as it removes wrongly based assumptions and expectations, and end-user can decide why and for what purposes to use the service, or not to use it at all.

And now I must confess that obviously in Nokia we do have also those end-user terms and conditions, but our approach became a very different one from the existing ones. Clearly it would have been an easy way to simply “copy with pride” the already used types widely available online.

The following elements were taken into account when really starting from scratch, with common decision to question everything:

- 1 Universal terms or service specific terms – what activities should be covered
  - Does it make difference if end-user is just browsing, down/uploading or actually buying something?
- 2 Regional mandatory requirements
  - How to define “region” and are there any similarities globally?
- 3 Language variants
  - How to administrate language variations, should it be based on user’s home country (reflecting applicable law) or language preference?
- 4 Customer requested variants (if any)
  - What if operators want to have deviations for services they are offering directly or indirectly?
- 5 Services provided by third parties
  - What if third parties want to include their terms&conditions or demand separate agreement between them and end-users?
  - How to handle specific restrictions created by third parties’ own contractual commitments?
- 6 Access from a device or access from PC
  - Can end-users be treated identically notwithstanding is the entry point via mobile device (identifying piece SIM-card indicating country of residence) or via PC (IP-address)?

The overall goal was to create a framework and terms covering all activities in all regions in the world in a structured way, including internal guidelines and governance model for ongoing process of adding, modifying or removing services to be offered under Nokia brand.

To question everything we also wanted to raise these questions and to discuss them in very open and honest way across Nokia legal and business:

- 1 Are we trying to create instructions or limitations or both?
- 2 Are marketing and granting information the same thing or are they in conflict with each other?
- 3 Is the intention to create defence for ourselves (tapping in a trial at certain point and saying “we have this in the terms”) or inform our end-users?
- 4 Should we try to summarize and use abstracts or detailed caseology?
- 5 Is there something we want to hinder or block, or something we want to avoid or something we actually want to promote?
- 6 Can we even define any kind of risk level or balance with ISP and hosting providers, governments, international organizations?
- 7 Are we running a service or a society?

The last question refers to the dilemma of creating new “legislation” by form of agreement, or analyzing if such terms already exist, or trusting that there is sufficient protection, remembering that customer is always right.

### **3 On Governmental Authority and Sovereignty**

I’ve often told the following example, which is not invented, but a real incident:

When one of our services (couple of years ago) was at trial-stage, or so-called beta-offering, a Japanese businessman travelling in Germany happened to purchase an item from our online service using his company’s American credit-card.

Obvious questions are: where did the transaction take place? What law applies to that transaction?

Governments want to rely on their authority and law-making power in a certain country. In most cases the boundaries limit also other rights and regulations and form natural limits to that sovereignty. As people have physically moved, they also have entered another country’s power of legislation.

Internet is (almost) open to all, and most pages (internet “sites”) and services are available for those persons who enter them, if that person can just read the language of the site.

Mobile phone is as the name indicates, mobile. With roaming arrangements allowing people to use their devices in almost from any country, these modern nomads can access other services from their devices than merely those offered in your country of more-or-less permanent residence.

Due to understandably very domestic approach to rules and regulations that might be easily accessible only to domestic companies, there is a threat that this alone discriminate again foreign companies operating in that country. Here again, the very large companies have possibility to invest into acquiring local assistance and legal counseling to clarify the position and to understand the local requirements to operate in that area.

The rules of the game are called laws, regulations and recommendations. These rules are today made by approximately more than 180 parliaments<sup>1</sup>, some supranational legislators, and international organizations such as EU, UN, OECD, WIPO, NAFTA, ICANN and others.

It seems that the above-mentioned organisations are taking more power, perhaps for natural reasons as they exist in order to facilitate certain cross-boundary activities. It is advisable that local governments would not increase their role in governance of internet, but this certainly remains to be seen. The result depends on much greater issue, that of world either opening, or countries closing their boundaries in fear of losing that absolute sovereignty.

Within European Union (which obviously is already supra-national organ) there is a clear-spoken initiative to promote consumers' right to transparency of information, but even in EU that has been a challenging goal and the road has not been easy. It is easy to understand that within boundaries of a separate country with full sovereignty the temptation to keep control has more weight than demands for openness.

In this context it seems that Albert Einstein's quote is ever so topical "Nothing is more destructive of the respect of the government and the law of the land than passing laws which can not be enforced".

I argue that it is not exaggerating to state that creativity and human race's possibility to record our own experiences is endangered due to increasing censorship demands and down-right attacks towards human rights.

Trying to define, what laws and regulations are in fact applicable, it seems that even the guidance is geographical – that is simply the way the world has operated until end of the last century. Choice is wide and has following starting points:

1. Applicable law
  - Private international law
  - EU legislation (internal market)
2. Territoriality
  - Substantive domestic law
  - Territory or place where incident took place (place of wrong)
3. Jurisdiction
  - Criminal or civil
  - Personal
  - Subject matter based
  - Territorial
4. Enforceability
  - EU Law
  - International treaties
  - Public interest (?)

---

1 Inter-Parliamentary Union "www.ipu.org/english/parlweb.htm".

#### 4 Babel – Language Requirements for Services

The language requirement applies for a device offered for sale in a country or to a service offered to residents of that country. This article is not going to explain in depth, when a service is offered to a resident of a country. In short, typically a service is deemed to be offered in a country, if it is offered in a website with that country's suffix (.de, .fr, .uk) or service is payable with local currency. With Euro been adopted widely in Europe, this is not such a clear guideline anymore.

Language requirements can be divided into three categories based on possible consequence of not honouring them:

- 1 General principle of offering service and its terms in a language that a consumer will understand -> consequence being that terms and conditions are not binding under local applicable law, since consumer could not be required to understand them
- 2 A legal requirement to offer service only in local official language -> consequence being that authorities can block the offering of services and demand service provider to withdraw from the market
- 3 A penalty for not offering services in a local official language

The last one is applied for example in France (Loi Toubon)<sup>2</sup> and Portugal and can bring severe monetary damages to service provider. Under French law the penalty of approaching French consumer only in other languages than French can be very severe, rising to hundreds of thousands of Euros..

This all sounds very straightforward and understandable in the best interest of both the companies and consumers. However, there are certain peculiarities that can rise from this demand.

Let's assume that a service package is nicely translated into French, all content and applications are localised and terms and conditions are in French. At the last moment there is a possibility to add free-of-charge an extra application, but it is yet only translated into some 6 languages, none of which happens to be French. Can a company offer this additional goodie to French-speaking audience? Assuming that some of the customers could understand the use of it, even though content is only in for example English, German and Spanish? The risk is that if company makes a wrong guess, it can be fined to pay considerable amounts of money, if planned distribution is even ten thousand copies. So the risk is high for the company and it is understandably tempting to leave that application out of the package directed to French consumers. But one could argue that in fact there will be real discrimination coming from the fact of *not* having access to the offering that all others will have, merely because it is safer for the service provider.

---

2 “en.wikipedia.org/wiki/Toubon\_Law” full text in French. “www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000056163341&dateTexte=20100801”.



Another example could be a native English-speaker moving to Finland. The official languages are Finnish and Swedish, but there is no requirement to serve customers of other language skills only. If a company would like to be friendly and offer other languages for its customers coming from Finnish ISP or mobile operator description, that would mean yet another version of English terms (already for UK, USA, Australia, New Zealand, Ireland and South Africa etc), because the existing English language versions are written from the point of view that applicable law is of that specific country, such as Australia – not Finland. Is it misleading to give possibility for speaker of Turkish to read and agree on Turkish terms and conditions, if the actual applicable law in those terms is that of Turkey?

Looking outside of Europe, the legislation is also very fragmented. In South Africa there are 11 languages to take into account, and in India a “minor dialect” is something that “only” 15 million people are having it as their mother tongue.

## **5 Legal Competence and Age Limits for Services and Content**

This is an extremely wide and important topic that has severe practical challenges.

The first obvious question is to understand the age of being legally competent, namely qualified to enter into legally binding contracts in a specific country. As mentioned earlier, this issue is treated differently in “real” world, since anyone with cash money can typically purchase items from shops and such an agreement is considered legally binding.

Unfortunately it is not even just a question of verifying the legal requirements in a country for competence, since there might be varying age-limits concerning different services in a same country. In addition, certain content must be classified according to applicable age-limit, such as movies. What is a movie is a debatable question as well, and in many countries even short advertisement video-clips for otherwise innocent products are considered as movies and can be age-rated only by nominated authorities in that country.

The clearance process can be very slowly and costly, again adding one more reason for a company of limited resources to exclude this kind of services from their offering. If a service provider does not have adequate age rating declarations (physical stickers or printed information), products not fulfilling legal requirements can not be sold in that country.

To make service provider’s life bit more exciting there are countries, where only the distributor is entitled to apply for such age-rating classification, meaning that the actual service provider can not do anything to facilitate that process or participate into it, only wait in anticipation.

When in the end all pieces in a service offering are investigated and rated in a one single country, and the service provider can feel sufficiently comfortable of complying with local laws and regulations, comes the real challenge: How to ensure that the end-user is of over that defined age-limit? And who is responsible, if an underage user gets access to content that otherwise would be off-limits?

Service provider can certainly install obstacles into the service that one can bypass only by having certain information or, the most popular alternative, having access to a credit-card. In most countries credit-cards are only available to those of full capacity, but nothing tells to the service provider, if the person inserting credit-card information is in fact the real owner of that card, or has successfully pinched it from adult's wallet.

## **6 Licenses and Separate Permissions to Seller Entity/Service Provider**

The essential question in many legal challenges is, who is the actual service provider? The answer to this question defines also the party responsible towards the end-user.

However, countries take a pride of offering different approaches also to this innocently looking issue. There are countries, where only the mother-company can be the selling entity, and countries, where express regulation is that only the subsidiary operating in that country can sell anything, maybe only thru a joint-venture.

Having solved this question the service provider might run into other practical problems, such as: if only mother-company can sell and is therefore the selling entity in the country A, who can provide support and maintenance to the end-user in that country? If mother company has no independent presence, but all the prior business has been conducted via local legal entity that has fully operating support and maintenance network, must the mother company now enter the market also for the end-user support purposes – which support may be a mandatory requirement under local applicable legislation.

If there is in fact a chain of companies, providing each some different elements of a service, who is the service provider, in the meaning of that local applicable law? Again a question with no clear answer, but solved on case-by-case basis. It will be solved, but by whom and within what time-frame, depends solely on the circumstances in that specific country – again adding strain and loss of money and time for the service provider or providers, depending on the outcome.

## **7 King Content**

Besides merely offering access, there is really no online service without content. The responsibility of that content is one of the most widely debated at this very moment. One of the most massive law-cases ever around this topic, the one between Viacom and Google (YouTube) is an unhappy reminder of unclear legal status.

The responsibility for content can be based on two very different principles, as content can be either copyright protected or simply inappropriate or considered harmful.

Copyrighted content is protected for reasons to protect copyright-holders. Any service provider offering space for customer uploads intends that space for content that end-user either has created himself or has sufficient permissions or licenses to upload. There are safe harbour provisions protecting service provider, if other criteria is fulfilled. Monitoring is usually not advised, as it might break the safe harbour protection, based on the reasoning that when monitoring, one is also editing and making therefore choices what can stay and what needs to be removed.

The other harmful content needs exactly opposite approach. Under many local legislations certain type of content is considered harmful and service provider needs to take precautions to block such content. Typical examples are child-pornography, Nazism related material, extreme violence and such.

But here we must face again cultural differences to what is appropriate and what is not – and those differences are huge. Based on my extremely limited personal experience European countries are typically much more sensitive to violence than for any sexually explicit content, as in Asia culture is more tolerant for violence, but in some countries even a kiss between woman and man might be quite literally blasphemy. In United States almost any expressions must be tolerated under First Amendment, but in Thailand and other countries one might face a jail sentence for insulting the much respected royal family.

Frequently there are demands that in the end-user terms all illegal activities must be expressly prohibited, even though that request is typically a mandatory local requirement. It might sound odd that a company would refuse to block and/or forbid activities that are in non-compliance with any applicable law or regulation, as usually complying of laws is a self-evident requirement for any company. But taking into account the huge differences what is illegal under any possible regulation of a single country, and also that in a one country an activity that is mentioned as a basic right under UN's Human Right declaration might in that country be defined as a crime, it seems more criminal to globally block e.g. criticising the government in discussion forums in a decent way

Another demanding task is to acquire necessary permissions and licenses to any content. Many years ago when Nokia needed very first licenses to a music-track, engineers simply asked that “go and purchase it” for global usage, childishly thinking that music was just another piece of software or code.

It was soon found out that there is no one-stop shop, where from one could acquire global rights to any song. So the answer to the question “Where from do you buy a global license?” is “From nowhere.” There is not “a license” but a large combination of rights is needed.

The license systems have – again - been built on territories, where local organisations have authority to grant local licenses only, even when that content and users are moving daily cross the borders. This means that permissions and licenses must be acquired from different sources, all of which have their own business models, which all makes it very challenging to even understand what the final cost of any one single song is. This is another example of need for very wide resources to negotiate with all parties such as record labels, publishers, artists and collecting societies.

## **8 Navigare Necessare Est – Navigation and Maps**

At a single glance one is tempted to consider that a map should be quite a simple element compared to music tracks, games or similar software applications.

Maps have one very sensitive point, and I'm referring again to the vulnerable relations between countries. Maps describe borders, and the world is full of border disputes, meaning that drawing the line between two countries in a virtual world can always be seen as a political decision. This has led to a situation where there needs to be several variants of the same area map, once again meaning additional efforts, confirmations, cost and surveillance.

In addition maps tell where everything is, including another sensitive topic, namely such as army and defence locations. There are countries that forbid telling the end-user exact coordinates of their own location for security reasons, meaning that a service provider can kind of hint where that person is, but not to give exact location data.

Using location data is yet another painfully sensitive topic, and the legislators' attitude seems to depend sometimes more on the context than actual storage and protection of such data. For example there are services marketed for purposes of other people knowing precisely where the end-user is, such as emergency services or parents knowing their child's position.

When and how can end-user decide who gets access to your location data and for what reasons? Can the authorities get that access under legislation that is in conflict with the one of the country where the server holding the data is located?

It is obvious that end-user must understand what it really means to share your location data with other users, or perhaps other service providers, so that they can give you such useful information as weather in the place the user happens to be.

If, as it is customary, a specific consent is needed from the end-user in all situations where location data will be shared, this means on the other hand that a system is needed to acquire and store those consents and verify there is one, before end-user's location data can be shared or used. Also possible changes to the service offering must be informed and perhaps a renewed consent must be acquired. This all makes perfect sense, but means considerable resources and investment, coming again back to my point that only companies of certain size can successfully fulfil all requirements.

Authorities might make requests to get access to location (or other) data for the purposes of their own criminal or other investigations. These requests are very often in total conflict with the laws of the country where the server with desired data resides. Not giving an authority X from country A an access to data residing on servers in country B, means that one is in breach of country A's laws. On the other hand giving the access would mean that one is in breach of country B's laws strictly prohibiting any transfer of or access to the data in question. The result is that some country's laws are violated in any case.

## 9 Conflicts at EU-Level Legislation

European Union is in constant search of balance between harmonization and autonomy of country level legislators, taking into account the subsidiarity principle. It is therefore understandable that when a directive gives room for country-level implementation there will be different variations of how a member-country shall implement any given directive.

Contrary to still popular view, the overall aim in the charters of European Union has not been to harmonize legislation in member-countries. Since already in the Single European Act of 1986 the aim was to create a complete internal market area before 1992, it is clear that differences in member-country legislation to create obstacles for a one, cohesive market area. This is a fact that most businesses operating in EU market area have learned to cope with to some extent.

However, the situation becomes graver, if within European Union law there are flaws.

There has been vivid discussion on different legal websites<sup>3</sup> since Italian court convicted Google's three executives, including Chief Legal Officer.

The case concerned a video-clip posted on the Italian site of Google Video, in year 2006. In this video an autistic child was harassed and bullied by other students in school. The video-clip was approximately two months visible at Google's Italian site.

It seems that users of the site had posted comments to the very page that contained video demanding the video should be removed, but without any reactions from Google. This is not that surprising, since typically this kind of services consist of thousands, if not tens of thousands video-clips, all with the space reserved for comments from other users.

Later Italian police sent a formal notice to Google, which according to its own words, removed the video within hours from receiving such notice from the police.

Do the comments from the end-user make an official take-down and remover request, an effective form of notice? It seems that E-commerce Directive does not give any guidance here.

What about Safe harbor protection under the E-commerce Directive, why were those not sufficient in this Italian case to protect Google against accusations?

Google claimed that "European Union law was drafted specifically to give hosting providers a safe harbor from liability", this under further conditions that if a notice is made about harmful content, the hosting provider shall remove any illegal content without delay.

This is indeed the case, and the entire Safe harbor concept was created in 2000, partly to response to a case in Germany.

A German court convicted in 1998 an executive of CompuServe Company, as their service allowed German internet users to access web-pages that contained

---

3 Article and analysis written by Struan Robertson from Pinsent Masons law office at "www.out-law.com/default.aspx?page=10805"

illegal content such as pornography. This decision was overturned in appeal court, and influenced deeply the safe harbor provisions to find their place in a proposal for E-commerce Directive.

This seemed to have made clarification for the internet service providers and giving them protection against their own users.

There seems to be, however, a serious flaw in the E-commerce Directive. The Article 1 (5) states very clearly that the Directive does not apply to those questions that are related to information society services covered by Directives 95/46/EC and 97/66/EC.

The more familiar name for the first one is Data Protection Directive, and the second has been replaced by what is known now as Electronic Privacy and Communications Directive.

This seems to indicate clearly that safe harbor provisions do not offer protection, if the case is about privacy and data protection. Exactly what was the case in Italy against Google. The court decision was based on data protection law of Italy.

More speculation has now been going around, why the E-commerce Directive excludes privacy and data protection. Was the intention to have separate protection clauses under those other directives, maybe with different conditions? Nobody has yet answered.

This scenario is again dependant on which country one is arguing it about. In UK the implementation of Data Protection Directive has been much less strict than in Italy and consequently the outcome of the case could have been different on these grounds.

There seems to be a touching consensus that safe harbor principle is crucial for the operation of internet services. Otherwise the service providers would be solely responsible instead of the persons actually and directly responsible for their own actions.

It also seems that there is an urgent need to either remove the reference to privacy and data protection directives from E-commerce Directive, or then add relevant safe harbor clauses into the privacy and data protection directives.

## **10 Conclusion**

There have been recent cases where courts have not enforced consumer terms and conditions on the grounds that they were too long and complicated. I personally welcome this approach and sincerely wish that this would lead way to clear and well-structured terms for online services that are written for the consumer and not for the judges, to be referred to in court cases.

However, the current fragmented legislation drives service providers to get the needed protection by writing all possible scenarios into terms and conditions. The fragmentation is not due to the fact of having almost 200 countries using their very long traditional right to legislate within their territory. The most confusing fragmentation comes from the fact that rules have been written to different streams of activities that are all converging into one offering, consequently leading to situation where several conflicting laws could be applied to the same service offering.

The service provider has no means to understand what law is applied to such converged package, since even the local authorities and government is arguing over this point. Still, a large multinational company probably has much better resources to made educated guesses than the consumer, customer, and the end-user, all who are financing this business out of their own pockets.

A consumer, who has tried out and purchased maybe few different devices and a collection of services/applications/software to run on them, has most likely already agreed to tens of very different sets of terms and conditions governing his/her usage of these packages. I am very much afraid they do not have a clear understanding what are the applicable rights and obligations, if any dispute would arise.

I am trying to point out, that neither the consumer nor the service providers can understand the consequences of their actions.

In my simple mind that is what legislation is all about: providing rules so that everyone can understand, estimate and trust that certain behavior has certain consequences, the very basics of causation principle.