Provider Liability

- A Comparison between American and German Law -

Author: Manfred Mieskes

Table of Contents

List of Abbreviations

EGG	Bill on legal framework conditions for electronic commerce (Elektronisches Geschäftsverkehrs-gesetz).
GG	Basic Law (Grundgesetz).
IuKDG	Information- and Communication-Services Act (Informations- und Kommunikationsdienstegesetz.
MDStV	Interstate Mediaservice Agreement (Mediendienstestaatsvertrag)
s	Section
StGB	Penal Code (Strafgesetzbuch).
TDG	Teleservices Act (Teledienstegesetz)
VwGO	Regulations governing administrative courts (Verwaltungsgerichtsordnung)
VwVfG	Administrative Procedure Act (Verwaltungsverfahrensgesetz)

Provider Liability

- A Comparison between American and German Law -

A. Introduction

The liability of Internet providers is perhaps the most controversial issue to emerge from the law of cyberspace. Should providers be treated as electronic publishers and thus made directly liable for all infringing gigabytes, which flow through their servers? Or are they merely the postmen of the Internet, common carriers exempt from all liability? As always in the realm of the law, the answer lies somewhere in the middle.
The purpose of this essay is to provide a comparative analysis of the American and the German approach to provider liability in form of an overview.

Internet is a booming new market. The turnover for goods and services is expected to rise from 70 million to 3,3 billion Euros in Europe.[1] A study of the American ministry of commerce reveals that the electronic commerce in the year 2002 will exceed 327 billion Dollars.[2] Probably, Internet providers will grow with these figures and will become a major power in the economy. Therefore, the issue of civil and criminal liability of Internet providers has a considerable economic importance. Seeing that the legal general framework has a central role for investments, increased provisions for liability would lead to a shift of the business activities to a country where the legal provisions are more obliging. This is the reason why there must be found not only a technically sensible -and legally appropriate- but also a global solution if distortion in competition and a competition for the best location shall be prevented.
This essay will focus on "true intermediaries", i.e. providers that are instrumental in transmitting and disseminating third party content, but neither initiate nor decide to disseminate a particular material. Currently, various types of providers are involved in delivering content to users. Typically, if a work is made available in the Internet a chain of intermediate providers are involved. Having acquired an

[1] See **Sieber**, Die Verantwortlichkeit von Providern im Rechtsvergleich, Zeitschrift für Urheber- und Medienrecht 1999, p. 196 (p. 196).
[2] See **Ibid**.

account with a hosting service provider, an information provider will upload web pages onto his web site which is physically located on the host's server. Through the storage on the server the uploaded documents become instantly available to everyone who has access to the World Wide Web. An access provider provides access to the Internet. On the way from the host to the access provider to the end user, the transported documents pass through the infrastructure of a network provider who provides the physical facilities to transport the information and transmits and routs it to the particular recipient. Nowadays it is almost common that a single company provides all of these services.

This essay is structured as follows. First, section B will examine the civil and criminal liability under German law. Thereafter, in section C the liability under American law will be presented, in section D the order to block access to information of two nazi pages in the USA –which was ordered by the district government of Düsseldorf- is analyzed under German and American law. Finally, a number of conclusions will be presented in section E.

B. Civil and Criminal Liability under German Law

I. Applicable Acts and Roots

For applying the right act, one has to divide between tele- and mediaservices. Teleservices are electronic information- and communication services, which are meant for individual use[3], e.g. access provider, electronic banking, databases, e-commerce and other services with individual aspects. They are under the federal competency according to Art. 73 GG; thus the Teleservices Act (TDG) applies to these services. Mediaservices are aimed for the general public[4]; e.g. online-newspapers, -magazines, -presentations of companies and editorial newsletters. The federal states have the competency over the mediaservices, Art. 75 Nr. 2 GG, and thus the Interstate Mediaservice Agreement (MDStV) must be applied. Many online services are both teleservices and mediaservices -such as Yahoo, which offers news, e-commerce and e-mail services. In that case both acts can be applied depending on the issue. But a differentiation between these two acts is

[3] See **Schmitz**, TDDSG und das Recht auf informationelle Selbstbestimmung, 3rd part, A II 2 b).

[4] See **Ibid.**

unproblematic because the provisions have almost the identical wording. Therefore, I want to focus this essay predominantly on the teleservices and thus the TDG

Germany has enacted the TDG through the Multimedia Act of 1997 (IuKDG). The act intends to regulate liability horizontally i.e. it's rules apply to the full range of liabilities resulting both from civil and criminal law. A special feature of this act is the fact that it acts as a filter. Only if the requirements of the act are met, may a court consider whether the provider is liable under civil or criminal law.[5]

The last amendment of the TDG was due to the E-Commerce Directive in January and in form of the bill on legal framework conditions for electronic commerce (EGG). Surprisingly, the liability rules of the directive were modelled upon the German Multimedia Act in that they deal with liability in a horizontal manner and serve as a filter as mentioned above. The Interstate Mediaservices Agreement entered into force in the same year as the TDG, in 1997 and some of its provisions provide requirements which have to be met in order that a mediaservice is liable under criminal law. Like the TDG it is also used as a filter.

II. Liability

Basically three types of providers are distinguished: content or information provider, access provider and host provider.

1. General Principles

Not surprisingly, content provider which offer own information are fully responsible for the content they disseminate and the general laws apply in full under s 8 I TDG and s 5 I MDStV. Sources of liability can be e.g. breach of warranty, product liability, infringements of trademarks, -names, -rights of personality, -copyrights, -data protection, child pornography, pornography, hate- and racist speech.

An important feature of the TDG is the fact that providers are not obliged to supervise information they have transmitted or stored or to research to determine circumstances that indicate an illegal activity according to s 8 II 1. sentence TDG. But obligations to remove or block the use of information under binding law

[5] See **Hoffmann**, Zivilrechtliche Haftung im Internet, MMR 5/2002, p. 284 (p. 285).

remain unaffected even if the provider is not responsible pursuant to sections 9 to 11 of the TDG under s 8 II 2. sentence TDG. This regulation concerns only obligations, which are detached of the fault und thus cannot be applied for criminal liability.[6] Therefore, civil and public law rights of forbearance can be filed even if the provider is liable under the TDG.

2. Transmission of Information (Mere Conduit)

Access provider are totally excluded from liability for third-party information, if they have not selected the addresses of the information that has been transmitted and not selected or modified the information that has been transmitted under s 9 I Nr. 2,3 TDG and s 5 III MDStV. Liability from the act of temporarily copying in the course of the provision of access is also excluded from liability, s 9 II TDG. Additionally, providers are not liable for routing according to s 9 I Nr. 1 TDG, i.e. the operation of computers which navigate the data between the sender and the recipient.[7]

Relating to the liability of access provider I would like to present a famous court decision. In May 1998, Felix Somm, a former managing director of Compuserve's German division was found guilty of violating the German Penal Code under sections 184 III Nr. 2, 11 III, 13, 14 I Nr. 1, 25 II, 52 StGB because he had made illegal pornographic Usenet news-groups available to Compuserve's German users.[8] The Bavarian court ruled that Compuserve Germany, a full subsidiary of Compuserve US, which routed traffic to the latter's servers, could not apply for the limitation in the Act open to access providers, because access to the Internet was provided by the parent company, and not by Compuserve Germany. At that time the "routing provision" of the new s 9 I Nr. 1 TDG was not expressly named in the former s 5 III TDG. The court ruled that the German subsidiary should be regarded as a hosting service provider. Sufficient knowledge which was required under the old TDG in s 5 II TDG was found on the basis that a provider who hosts news groups with names as "alt.sex" and "alt.erotica" can be presumed to know of the fact that pornographic material is available on its servers. Thus knowledge of an actual message or of particular material is not required. Finally, it would be

---

[6] See **Sieber**, Rechtliche Verantwortlichkeit im Internet, MMR-Beilage 2/1999, p. 18 (p. 25).
[7] See **Hoffmann**, Zivilrechtliche Haftung im Internet, MMR 5/2002, p. 284 (p. 286).
[8] See AG München, MMR 8/1998, p. 429 (p. 429).

technically feasible and could be reasonably expected to block access. The Compuserve decision has been met with severe criticism, both in legal magazines and the general press, and even by German officials.[9] But in November 1999, the Bavarian OLG München[10] overturned the Somm verdict, ruling that Somm could not have reasonably done more about the newsgroup than requesting from the parent company, which housed the newsgroups on its servers in the US, to block access to them and that s 5 III TDG (old TDG section) which excludes liability of access providers, is also applicable to Routing.

3. Intermediate Storage to Accelerate Data Transmission (Caching)

According to s 10 TDG providers are not responsible for automatic, intermediate storage for a limited period of time which is carried out solely to enhance the efficiency of the transmission of third-party information to other users upon the latter's request. This is the typical constellation of servers which copy whole areas of hard disc content of foreign servers (Mirror-method) or save pages which are called away/are accessed by users (Proxy-Cache-Server).[11]

4. Storage of Information (Hosting)

Providers who store third-party information are not liable if they have no actual knowledge of illegal activity or information and in case of claims for damages if they are not aware of facts or circumstances from which the illegal activity or information is apparent (gross negligence) under s 11 Nr. 1 TDG and s 5 II MDStV. Moreover, providers (solely teleservices) must act expeditiously to remove or to disable access to the information as soon as they become aware of such circumstances, s 11 Nr. 2 TDG. Another prerequisite was stated in the former s 11, which was s 5 II TDG and requires that preventing further dissemination is technically possible and can be reasonably expected by the provider. This former written prerequisite is still an unwritten prerequisite for teleservices and a written prerequisite for mediaservices according to s 5 II MDStV. When the word information is used in the TDG it constitutes also

[9] See **Ibid**, (p. 438).
[10] See OLG München, MMR 10/2000, p. 617 (p. 617).
[11] See **Hoffmann**, Zivilrechtliche Haftung im Internet, MMR 5/2002, p. 284 (p. 287).

copyrights (including software) and trademarks.[12] Recent decisions, which have not applied this provision for copyright-protected music (AOL-judgement - Midi-Files)[13] and for trademarks (Internet auction – Ricardo)[14] are thus untenable with the new legal status. Examples for hosting service providers are web-hosting services, providers who offer internet auctions e.g. Ebay or Ricardo and services where news-groups or chat-forums are offered for its' users.

5. Unregulated Areas

Hyperlinks and search engines are not regulated both in the TDG and the MDStV. Art. 21 II of the E-commerce Directive states that a regulation of these both areas is not intended yet. The German legislator takes a similar view to this issue and has not regulated these topics through the EGG, which amended the TDG this year in January. Therefore, it is not possible to make use of the provisions in the sections 8-11 TDG by analogous use –as it was done with the former law in s 5 of the old TDG.[15] Applying the old law the OLG Köln permitted a search engine – viewing it as an access provider-, which searched for newspaper articles in the net and made them accessible at their own homepage.[16]

Hyperlinks connect the whole web by linking one page to another. Normally the person/entity who installs a hyperlink is not liable for the illegal content of the linked web side. An exception would be e.g. if the link aims directly at a well-known nazi site and the title of the link is also obvious. Moreover, the German courts have found that deep links[17] and inline links[18] are inadmissible. A deep link connects a website by going round the homepage directly to the website without the knowledge of the user. Through an inline link a user does not recognize that the information he actually sees is from another web site.

---

[12] See **Ibid,** (p. 288).
[13] See OLG München, MMR 2001, p. 378 (p. 378).
[14] See OLG Köln, MMR 2002, p. 110 (p. 110).
[15] See. **Spindler**, Das Gesetz zum elektronischen Geschäftsverkehr, NJW 13/2002, p. 921 (p. 924).
[16] See OLG Köln, MMR 2001, p. 387, (p. 387).
[17] See OLG Celle http://www.flick-sass.de/links03.html.

[18] See OLG Düsseldorf K&R 2000, p. 87 (p. 89).

C. Liability under American Law

The sources of provider liability are based upon federal – and states acts and case law. This essay will focus on the federal law and view important judgements.

I. Civil Liability

Similar principles as in Germany and the EU are being applied also in the United States of America. Many individual acts based upon judicial precedents regulate the liability. All these acts are collected and united in the United States Code (USC) in particular theme-based chapters. For the civil liability three acts are important to know: the Communications Decency Act (CDA) which can be found in 47 USC s 223 (a) (1) (B) (ii), (d), (e) and s 230 (c) (1), the Child Online Protection Act (COPA) in 47 USC s 230 (d), s 231and the Digital Millennium Copyright Act (DMCA) in 17 USC. At the beginning of this analysis it must be mentioned in advance as a general rule that content provider are liable for their information under general law.

1. Communication Decency Act

According to 47 USC s 223 (a) (1) (B) (ii) it is prohibited to initiate the transmission of any comment, request, suggestion, proposal, image or other communication which is obscene or indecent if the provider knows that the recipient is under 18 years of age and shall be fined under title 18 USC or imprisoned not more than two years or both. Furthermore, it is forbidden with the same sanction as mentioned above to send offensive material to persons under 18 through an interactive computer service that contents patently offensive, sexual or excretory activities or organs under 47 USC s 223 (d) (1) (B). These prohibitions apply to all types of providers. But 47 USC s 223 (e) excludes access providers from liability if they have violated subsection (a) or (d) (see above). Of course there is a exemption of this general rule; in case of a conspiracy between the access provider with an entity actively involved in the creation of communications that violates the above mentioned section under 47 USC s 223 (e) (2) –which is similar to s 9 I sentence 2 of the German TDG. Additionally, access and hosting provider are not liable because according to 47 USC s 230 (c) (1) they shall not be

treated as the publisher or speaker of any information provided by another information content provider. Another important provision is supplied by 47 USC s 230 (c) (2) (A) which states that no provider is liable on account of any action voluntarily taken in good faith to restrict access which is considered to be offensive (Good Samaritan provision). This section was introduced in order to prevent providers to be held liable who tried blocking access to offensive material (e.g. through a directive and filter software for users) as it happened in the case of Stratton Oakmont Inc. v. Prodigy Services Co.[19]. The leading case on this rule of federal immunity is Zeran v. America Online Inc.[20], where the court found that Congress made a deliberate policy choice to immunize those access and host provider from tort liability even if they have knowledge of the illegal content by information of users.

2. Child Online Protection Act

An obligation for the provider (interactive computer service) to notify the customer that parental control protections (such as filter services) are commercially available arises from 47 USC s 230 (d). The s 231 of the COPA is not in force yet due to constitutional doubts.[21].

3. Digital Millennium Copyright Act

The DMCA is intended to provide a limited safe harbour for online service providers with respect to copyrighted materials passing through, cached in, residing on, or linked to pages on their systems if specific requirements are met. A short overview is outlined below.

An access provider is not liable according to 17 USC s 512 (a) -similar to s 10 TDG- and an intermediate storage (caching) bears no liability, 17 USC s 512 (b). If a hosting provider wants to escape from liability he must show that he had no actual knowledge of the infringement of copyrights or that he was not aware of fact from which infringing activity is apparent, 17 USC, s 512 (c) (1) (A) (i), (ii).

---

[19] See **Hein, Davies**, Haftung für fremde Inhalte im Internet nach US-Recht, MMR 12/1998, p. 627 (p. 628).

[20] See Zeran v. America Online Inc., http://www.law.emory.edu/4circuit/nov97/971523.p.html.

[21] See Doe v. America Online, http://www.gigalaw.com/library/reno-aclu-1997-06-26-p1.html.

Moreover, the hosting provider must expeditiously block access to the information if he receives a notification of information by a third party, (iii), with the required content of 17 USC s 512 (c) (3) (A) –which must basically proof the copyright infringement.

II. Criminal Liability

1. Federal Law

Section 223 (e) of chapter 47 USC is both applicable to civil and criminal law. Other federal acts don't exist at the moment, but there is a legislative bill, "The Online Liability Standardisation Act", which is intended to treat service providers in the criminal law in the same way as in civil law. It shall protect service providers from criminal liability for illegal activities of third-party users, as long as the service provider did not create the content and its senior employees were unaware of the activities.

2. Case Law

There are hardly any court decisions where service providers were convicted due to infringements of criminal law. But the judgments from the civil liability of Internet providers may be important for the criminal liability too. The principle that publishers and distributors of third-party information are not liable, which was held in the above-mentioned Zeran decision and many others, was codified through the CDA and derives from the leading case Smith v. California, which was a criminal case. In the Smith case a bookseller was held not guilty for the illegal content of a pornographic book he sold because otherwise the freedom of press, protected by the first Amendment, would have been under danger. Therefore, this principle should be applied also to Internet providers, and it will be applied in case the proposed bill is going to be accepted by Congress.

D. The Order to block Access to certain Web Sites

The head of the district government (Bezirksregierung) in Düsseldorf -Mr. Jürgen Büssow - has ordered 90 access providers to block access to 2 nazi web sites in

the USA through an administrative act (Sperrungsverfügung)[22] at the 13th February 2002. The nazi web sites located in the USA are www.stormfront.org and www.nazi-lauck-nsdapao.com. Currently, administrative proceedings reviewing an individual administrative decision upon protest by the parties aggrieved take place. Through a protest to set aside the order, the legal issues will be analysed in the following pages.

I. Protest against the Order to block Access to the Stormfront and the Nazi-Lauck Web Site

The protest against the order to block access to the two nazi web sites could be successful if the order is admissible and reasonably justified.

1. Admissibility

a. Public Course of Law and Permissibility

The public course of law is given under s 40 I VwGO (analogous use). Furthermore, the protest is permissible according to s 68 I VwGO because the order is an administrative act, s 35 VwVfG. The protest is aimed to set aside the order because it is an administrative act, which burdens the addressee.

b. Authorisation to Protest, Time Limit, Form and Public Authority deciding on Protest

According to s 42 II VwGO (analogous use) a protest is only admissible if the entity that files the protest shows that the administrative act violated his right. This requirement is given through the theory of the addressee. The time limit for the protest is a month –because an instruction about legal remedies available was included in the order-, the public authority deciding on the protest is the district government (Bezirksregierung) of Düsseldorf because it ordered to block access and the protest must be written under s 70 I sentence 1 VwGO.

Intermediate result: The protest would be admissible.

---

[22] The order to block access (Sperrungsverfügung) can be found at: http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/THEMEN_Beitrag_druckbar.html?query=THBTR.ID%3d7072

2. Reasonable Justification

According to s 113 I VwGO (analogous use) a protest is reasonably justified if the administrative act is illegal and the protesting person's rights are therefore violated.

a. Legal Basis

The legal basis for the order is s 18 II, III MDStV in connection with s 1 II OBG because of illegal contents under s 8 I MDStV.

b. Formal Lawfulness

It is questionable whether the public authority (Bezirksregierung Düsseldorf), which ordered the blocking of access, had the competency. The public authority could have the competency because it is the competent public authority for the protection of children and young people under s 18 I MDStV in connection with s 12 OBG and therefore supervises the keeping of the provisions in s 8 and s 9 I MDStV. But it is doubtful, whether the MDStV is applicable to access provider. The two nazi web sites as a content provider infringed the German Penal Code and are liable under s 5 I MDStV, but because they are located in the USA the district government cannot order them to block the websites, thus they ordered the access provider in Germany to block access under s 18 III MDStV. This provision contradicts to s 2 II Nr. 4 MDStV which states that services which transfer data – which are access provider- and services which are meant for individual use are not mediaservices. This is a contradiction, which must be solved by the legislator through an Amendment; until then the district government (Bezirksregierung) has the competence for that order.

Intermediate result: This leads to the result that the protest is formally lawful.

c. Material Lawfulness

According to s 18 III MDStV the public authority can order the access provider to block access if measures against the content provider have no success. These measures against the owners of the websites are hardly enforceable because of the difficulties of enforceability of foreign court decisions in the USA, which has

shown again the recent Yahoo decision.[23] There is no doubt that the public authority has to act because of s 18 II MDStV when s 8 of the MDStV is infringed. Both mentioned websites are under s 8 MDStV illegal because they infringe the following provisions of the German Penal Code:

- s 130 I,II StGB because incitement of the people is given
- s 86 a StGB because of use of symbols of unconstitutional organizations
- s 86 I Nr. 4 StGB because means of illegal nazi propaganda are made publicly accessible

Moreover, the websites glorify war and infringe s 8 I Nr. 2 MDStV and are suitable to endanger children and young people under s 8 I Nr. 3 MDStV.

But another prerequisite states that blocking must be technically possible and appropriate, s 18 III MDStV.

The offered possibilities by the public authority are *exclusion of domains in the Domain Name Server (DNS)* – by this way inquiries to a certain web site are send to an invalid IP-address-, *usage of a proxy server* and *exclusion of the Internet Protocol (IP)-Address through blocking in the Router*. Routing represents interfering with the routing tables of the routers. This can be achieved by discarding all packet bound for certain destinations when they arrive at the router (grounding the route) In that way entire computers are made inaccessible disregarding the fact whether legal or illegal content is stored on the computer. By using a proxy or other firewall software, selective blocking at the level of individual pages can be achieved. As a rule, the operation of such a system is very cumbersome and costly and therefore not feasible. The other two possibilities are technically feasible.

The blocking must also be appropriate. Analysing this, the financial burdening and the threat for the object of legal protection must be weighed up. On the one hand these web sites with their inhuman content can have a negative influence on children and young people and can be viewed thus as a threat for our society. But on the other hand if this order is lawful, other orders to block access to the thousands of web sites with illegal content would be such a burden for the provider, because he would be obliged to administer the old- and complete the new web sites which have to be blocked, that his services would be slowed down considerably and his expenses would rise to incredible high sums. Such

[23] See District Court of California, Cri 1/2002, Yahoo! Inc. v. La Ligue Contre Le Racisme, p. 13.

interventions are a threat to the economic power of a company and can lead even to the ruin.
Therefore, the order to block access is partly not feasible and not appropriate. This alone would lead to the result that the order to block access to the two named web sites is materially unlawful.

The order must be proportional as well; otherwise it is materially unlawful (Although it is already materially unlawful I proceed with analysing the order). In order to fulfil this requirement the measure must be suitable by leading to the intended success. Exactly this is highly questionable in this case. The reason lies in the fact that users can evade blocking easily.

1. The user can install another DNS-Server in his computer without much effort and knowledge or just change his Internet provider; he could even take a provider from abroad. With this method the exclusion of domains in the DNS could be by-passed.
2. Mirroring is another way of by-passing the order. Mirroring takes place when the whole content of a website is saved by another. Search engines do exactly this every day in order to be able to present quick and the best search results. Thus the usage of a proxy server and routing would not lead to the intended result. But ordering the search engines companies such as Google to delete these data would lead to catastrophic consequences for the new economy in Germany.

Therefore, the order is partly not feasible, not appropriate and not proportional, which leads to the result that the order to block access to the two named web sites is materially unlawful.

d. Subjective Violation of the Law

Finally, the protesting person's rights must be violated. This prerequisite is also given by an infringement of Art. 14 I GG due to a particularly aimed intervention in the commercial enterprise and a violation of Art. 12 I GG –occupational liberty. Moreover, Art. 2 I GG –general freedom of action- can be infringed as well.

<u>Result:</u> The protest has a good perspective to be successful because the order is reasonably not justified due to the material unlawfulness.

Comment: Even if the public authority does not have the competency and the TDG must be applied, obligations to block access under s 8 II sentence 2 TDG relate solely to obligations which are detached of the fault and therefore not for criminal liability (see B II 1). S 8 II sentence 2 TDG would not represent a legal basis for this case. Another issue, which has to be thought about, is a possible violation of Art. 5 I GG, which constitutes the freedom of expression. This right could be endangered through a possible censorship in case the order must be enforced. From my point of view, the user should decide whether to enter or not to enter a particular homepage. The protection of children could be achieved through filter software which can be installed by their parents and, which ensures safe surfing in the Internet for children. Additionally, the free movement of services under s 49 EC-Treaty could be infringed because the order could be a forbidden restriction in the common market in case that a foreign EU competitor enters the German market in order to offer it's provider services.

II. American View

In the vast majority of cases online hate speech –which can be found on the web sites of Stormfront and Lauck- remains protected under the First Amendment of the American Constitution, which constitutes the Freedom of Speech. But there are legal remedies available when hate speech crosses the line into threats, harassing speech, incitement to violence and group libel.

Threats are generally defined "as declarations of intention to inflict punishment, loss, or pain on another, or to injure another by the commission of some unlawful act"[24]. Nevertheless, as a requirement both threats and harassment must be directed at specific individuals in order not to be protected by the first Amendment. This principle was confirmed by the landmark decision of US v. Watts[25]. Thus blanket statements, which express hatred towards a racial group, cannot be considered to be hate speech or harassment.

Another unprotected activity is incitement to violence. The Supreme Court of the United States ruled in the Brandenburg v. Ohio case that there is a line between

[24] **Anti Defamation League**, Combating Extremism in Cyberspace, http://www.adl.org/Civil_Rights/newcyber.pdf.

[25] See Supreme Court of the US, US v. Watts, http://www.adl.org/Civil_Rights/newcyber.pdf.

speech that is "directed to inciting or producing imminent lawless action"[26] – which is not protected by the first Amendment- and speech that is not likely to incite such action. Still, this necessary standard is a high bar to meet and therefore, online hate speech will rarely be punishable under this criteria.
Online group libel, which are e.g. libellous hateful comments directed toward Jews or another racial group, is not an actionable offence. But if it is again directed toward a particular person, it is actionable under the law and not protected by Freedom of Speech.
Because the Stormfront and Lauck web sites fulfil none of these requirements, these sites are protected under the first Amendment of the US. Thus in the USA an order directed to access-, hosting providers or to the owners of the content (Stormfront and Lauck) to shut down the web sites or block access is highly improbable.

The important difference between the American and the German law is that the German law protects also the freedom of speech under Art. 5 I GG but does not require expressly that threats, harassment, incitement to violence and group libel must be directed toward a particular person in order to be illegal. One reason of the different treatment and approach is probably the dark history of Germany during the Second World War with the mass extermination of Jews by the Nazis.

E. Conclusion

As this study has demonstrated, legislatures and courts in America and Germany have dealt with the problems of online liability in remarkably similar ways, based on general principles of common or civil tort law and criminal law. The basic rules are roughly the same:

- Content providers are liable under the general law.
- Access provider are exempt from liability
- and absent knowledge or awareness, hosting providers are not liable for monetary relief.

[26] Supreme Court of the US, Brandenburg v. Ohio, http://www.bc.edu/bc_org/avp/cas/comm/free_speech/brandenburg.html.

If the OLSA passes Congress even the limitation of the criminal liability of Internet providers will be similar.

As a bilateral rule one could assume that Americans are in general more concerned about pornography in the Internet and Germans are more concerned about online hate- and nazi speech.

If an international initiative were to be contemplated, the US/German consensus would appear to be the obvious point of departure.

Reading List

Anti Defamation League	Combating Extremism in Cyberspace, http://www.adl.org/Civil_Rights/newcyber.pdf
Düsseldorfer Bezirks-regierung	Sperrungsverfügung/order to block access, http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/THEMEN_Beitrag_druckbar.html?query=THBTR.ID%3d7072
Hein, J. Werner; Davies, Mark S.	Haftung für fremde Inhalte im Internet nach US-amerikanischem Recht, in: Multi Media Recht 12/1998, p. 627-630.
Hoffmann, Helmut	Zivilrechtliche Haftung im Internet, in: Multi Media Recht 5/2002, p. 284-289.
Schmitz, Peter	TDDSG und das Recht auf informationelle Selbstbestimmung, 1. Auflage, München 2000.
Sieber, Ulrich	Die Verantwortlichkeit von Internet-Providern im Rechtsvergleich, in: Zeitschrift für Urheber- und Medienrecht 1999, p. 196-202.
Sieber, Ulrich	Rechtliche Verantwortlichkeit im Internet, in: Multi Media Recht – Beilage 2/1999, p. 20-30.
Spindler, Gerald	Das Gesetz zum elektronischen Geschäftsverkehr, in: Neue Juristische Wochenschrift 13/2002, p. 921-927.