1-1-1998

The New German Internet Law

Lothar Determann

Follow this and additional works at: https://repository.uchastings.edu/hastings_international_comparative_law_review

Part of the Comparative and Foreign Law Commons, and the International Law Commons

Recommended Citation

Lothar Determann, The New German Internet Law, 22 Hastings Int’l & Comp. L. Rev. 113 (1998). Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol22/iss1/3

This Article is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings International and Comparative Law Review by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
The New German Internet Law

By LOTHAR DETERMANN

Table of Contents

I. Relevance of Foreign Law to Internet Users and Providers..116
   A. Early Precedents.................................................................117
   B. Germany v. Felix Somm..................................................119
   C. Extraterritorial Application of National Laws and Its Limits.................................................................124
      1. General Statutory Provisions on the Applicability of German Criminal Law........................................124
      2. International Law Limits on National Jurisdiction to Prescribe..........................................................125
      3. Concept of Territoriality Imposes Few Significant Limits in Cyberspace...........................................126
   D. Potential Consequences for Private Users..............................................128
   E. Conclusion.............................................................................129

II. New German Statutes Governing Online Services ..........129
   A. Range of Applicability of the Federal Law (IuKDG) and the Uniform State Codes (MDStV) on Internet Services .........................................................................................................................130
      1. General Federal Rules for All Online Services, Specific Federal Rules for Tele Services and Specific State Rules for Media Services .........................................................130
      2. State and Federal Legislative Powers in Germany and the Legislative Powers of the European Community.................................................................................................................................131
         a. Vertical Separation of Powers in Germany ..........131

Dr. jur. Lothar Determann has been teaching public law at Freie Universitaet Berlin in Germany since 1994. The author would like to give special thanks to Kathleen A. Weaver, attorney at Baker & McKenzie, San Francisco for valuable remarks and comments on earlier drafts of this article. All opinions and errors remain the sole responsibility of the author.
b. Most Subjects Fall Under Federal Legislative Competence ..................................................132
c. State Law Governing the Press and Other Media .....................................................................132
d. Precedents ...............................................................................................................................134
e. European Community Remained Inactive .............136
f. Compromise Under Political Pressure .................136
3. Statutory Definitions of Broadcasting, Media Services and Tele Services ................................138
a. German Federal Statutes Apply Not Only to Interstate and Foreign Communication ..........138
b. Few Technical Differences Between the Legal Categories ....................................................138
c. Vague and Similar Legal Definitions .................................................................138
   i. Tele Services .......................................................................................................................139
   ii. Media Services ...................................................................................................................139
   iii. Broadcasting and Cable Television .................140
   iv. Critique .............................................................................................................................140
B. Rules of the New German Multimedia Law ..........141
   1. Providers and Users............................................................141
   2. Specific Content-Based Speech Restrictions on the Internet and Defenses ......................143
      a. No New Content-Based Speech Restrictions in the New German Federal Internet Law ..........144
         i. Extension of Existing Speech Restrictions ......................................................................144
         ii. Specifically: Racist Hate Speech ..................................................................................145
         iii. Obscenity .....................................................................................................................145
      b. References to Federal Law in the State Code ......146
      c. Speech Restrictions in the United States: The CDA .......................................................147
         i. Indecent Speech and the First Amendment of the U.S. Constitution ......147
         ii. Extraterritorial Application of the CDA .......................................................................148
      d. Conclusion and Comparison .........................................................................................150
   3. Specific Privileges for Access and Service Providers Regarding Secondary Liability ..........151
      a. Liability of Providers According to Federal Law ..............................................................152
         i. Service Providers ............................................................................................................152
In August 1997, new statutory rules aimed specifically at regulating Internet services and other online media came into effect in Germany. This article introduces these new rules and related consti-

1. Gesetz zur Regelung der Rahmenbedingungen fuer Informations- und Kommunikationsdienste [Statute on the General Conditions of Information and Communication Services] [IuKDG], v. 22.7.1997 (BGBI. I S.1870-1879); Staatsvertrag uber Medien dienste [State Treaty on Media Services] [MDStV], v. 20.5.1997 (Hessisches GVBl. I S.134, Berliner GVBl. I S.361). The new Internet law categorizes the different cyberspace players into “Content Providers,” “Access Providers,” “Service Providers” and “Users” (see infra Part II.B.1), and differentiates between “Tele Services” and “Media Services” (see infra Part II.A.1). As these terms are currently neither terms of the industry nor commonly or uniformly used expressions, they appear capitalized throughout this article.

tutional issues and compares them with their United States counterpart, the Communications Decency Act (CDA), which itself has been the source of much recent constitutional debate.

I. Relevance of Foreign Law to Internet Users and Providers

Due to the rapid pace of technological advances, such as satellite television, digital broadcasting and the Internet, public and private communications have become issues of increasingly international proportions. Unfortunately, the legal community moves much more slowly and, as a result, a comprehensive international telecommunication and media law does not yet exist. As a result, while a person may now potentially reach anywhere in the world, that person does so at the risk of running afoul of each recipient nation’s laws and standards.

The Internet allows millions of users to communicate with citizens and businesses all over the world. However, many such users

---


5. See Carl Benson et al., Computer Crimes, 34 AM. CRIM. L. REV. 409, 437-41 (1997); Ali Staiman, Shielding Internet Users From Undesirable Content: The Advantages of a PICS Based Rating System, 20 FORDHAM INT’L L.J. 866, 866 (1997) (citing a European Commission Green Paper regarding pornography on the internet which said, “We know that national regulation . . . is not enough, that European regulation is not enough. . . . We may need to have a world regulation of these matters.”).
never realize that they may become subject to foreign law and to the jurisdiction of foreign courts and government agencies without ever leaving home.

In the past, the international repercussions of private communications were not an issue of much practical relevance with respect to one-to-one communications, such as communications via mail, telephone and facsimile. Historically, most national courts and agencies generally respected the privacy of these types of direct communications. Such private communications were generally not monitored for potential content-based violations, such as prohibited obscene or defamatory speech. In the unlikely event that a violation in an international context was brought to the attention of a national court or agency by a citizen who was perhaps insulted or harassed on the phone by a foreign national living abroad, it would have been highly unlikely for any such court or agency to take action. Jurisdiction notwithstanding, proceedings and enforcing sanctions against foreign citizens living abroad was extremely difficult, if not altogether impossible in practice, and depended on the existence of and reciprocal compliance with respective treaties.

The advent of the Internet injected new considerations into the realms of communications law. First of all, most of the communication options via the Internet are public, such as, home pages, bulletin boards and newsgroups. Consequently, they can be monitored by most countries’ government agencies without violating their respective privacy laws. Second, the globalization of commerce and commercial enterprises provides agencies and courts with new and expanded enforcement options.

A. Early Precedents

The first Internet cases that introduced problems of interstate dimensions seem to have originated in the United States six to seven

---

6. The issue of personal and subject matter jurisdiction is not discussed any further in this article. For further discussion (in an inter-state context within the United States), see, e.g., American Network, Inc. v. Access Am./Connect Atlanta, 975 F. Supp. 494 (S.D.N.Y. 1997) and United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).


years ago. However, one of the first examples of the application of local statutes to communications with an international dimension seems to have occurred in Germany in 1995, before the new Internet law was enacted. It involved the German subsidiary of a corporation based in the United States.  

CompuServe Deutschland GmbH is a wholly owned subsidiary of CompuServe, Inc., a U.S. company. In 1995, the German subsidiary had approximately 170 employees and was engaged in marketing, sales, customer service and technical support for the U.S. parent company in connection with the Internet services provided by CompuServe, Inc. It participated in the distribution of contents from U.S. servers to German Internet Users by maintaining a dedicated phone line between the servers of its parent company and Internet gateways in Germany. In this manner, the German subsidiary facilitated the access of German Internet Users to servers operated by CompuServe in the United States. The German Internet Users did not contract with CompuServe Deutschland GmbH, however, but rather directly with CompuServe, Inc. which offered, among other things, access to contents on its servers. These servers were based and operated in the United States and contained, in addition to other things, video games and newsgroups with articles published by U.S. Internet Content Providers.

In December 1995, Munich law enforcement officials provided CompuServe Deutschland GmbH with a list of 282 newsgroups emanating from CompuServe, Inc.’s servers, each of which contained pornography involving children and extreme violence. The District Attorney notified CompuServe Deutschland GmbH that these contents were illegal, indicated the possibility of criminal sanctions and asked it to prevent further distribution. The director of the German subsidiary, Felix Somm, informed CompuServe, Inc. of the incident.


10. The following facts are reported in the decision of the Munich local court discussed infra Part I.B. See Amtsgericht Muenchen [AG Muenchen], in der Strafsache gegen Felix Somm wegen der Verbreitung pornographischer Schriften, Az. 8340 Ds 465 Js 173158/95 (May 28, 1998) [hereinafter AG Muenchen] (this decision has been published in parts after completion of this article in 1998 CR 500-05 and 1998 MMR 429-38); see also Staiman, supra note 5, at 891; Eric Berlin, CompuServe Bows to Germany, INTERNET WORLD, Apr. 1996 <http://www.internetworld.com/print/monthly/1996/04/news.html>; Ulrich Sieber, Strafrechtliche Verantwortlichkeit fuer den Datenverkehr in internationalen Computernetzen [Criminal Liability for Data Transfer in International Computer Networks], 1996 JURISTEN ZEITUNG 429.
CompuServe, Inc. blocked the 282 newsgroups shortly thereafter to avoid sanctions against its subsidiary. Thus, statements by U.S. citizens which were published on a server located in the United States and operated by a U.S. Service Provider were forcibly conformed to German law and standards of free speech. Since then, similar efforts have been undertaken by French and British government agencies.11

Although German law professors12 and politicians substantially criticized the proceedings of the Munich prosecutors described above, German district attorneys continue to similarly enforce German anti-pornography, anti-terrorist and anti-racist law against communications emanating from other countries. Moreover, German district attorneys caused Service Providers and their servers to be searched abroad, namely in the Netherlands and Austria.13 Following the events of December 1995, actions by CompuServe, Inc. led to proceedings against CompuServe Deutschland GmbH. Those proceedings resulted in Mr. Somm being the first convicted online provider in Germany (see Part I.B infra). Ironically, this occurred despite the fact that the Munich District Attorney requested an acquittal of Mr. Somm after the new German Internet law was enacted which, as they correctly assumed, applied retroactively and exempted him from criminal liability.

B. Germany v. Felix Somm

The court decision14 discussed below deals with events that occurred in 1996 after CompuServe, Inc. blocked certain contents rebuked by the Munich District Attorney in 1995. In order to avoid sanctions against its German subsidiary, CompuServe, Inc. blocked

---


12. Sieber, supra note 10; Eric Hilgendorf, Ueberlegungen zur strafrechtlichen Interpretation des Ubiquitaetsprinzips im Zeitalter des Internet [Considerations Regarding the Criminal Law Interpretation of the Principle of Ubiquity], 1997 NJW 1873, 1874.


the controversial newsgroups completely and worldwide, including in the United States. This block caused an uproar in the Internet community—especially in the United States—which impaired CompuServe's worldwide business.\textsuperscript{15}

In February 1996, in response to that uproar, CompuServe, Inc. again made the newsgroups in question accessible to Internet Users worldwide, including German Internet Users by necessity. The German subsidiary informed the Munich District Attorney that it deemed further blocking unnecessary because CompuServe Deutschland GmbH now offered a free filter program named "Cyber Patrol" to its customers. The company argued it had therefore taken all reasonable and acceptable steps to prevent minors from accessing illegal contents. The District Attorney did not agree because distribution of violent and child pornography to adults also violates German criminal law and formally filed a bill of indictment against Mr. Somm.

On May 28, 1998, the German criminal court of first instance in Munich, the Amtsgericht Muenchen, sentenced Mr. Somm, who had no previous police record, to two years of imprisonment, suspended during probation.\textsuperscript{16} The court held that Mr. Somm was guilty of thirteen counts of violating section 184 III of the German Penal Code (StGB)\textsuperscript{17} by intentionally distributing child, animal and extremely violent pornography, and that he negligently violated Section 21 III of the German Code on Youth Protection (GjS)\textsuperscript{18} by making video games rated PG-18 available to minors.

Throughout 1996, newsgroup articles containing pictures of children, animal and extremely violent pornography (as described in detail in the Munich court decision)\textsuperscript{19} continued to be available on servers operated by CompuServe, Inc. These materials were accessible to Internet Users worldwide. German Internet Users could gain access to these materials via the dedicated phone line and gateways oper-

\textsuperscript{15} See, e.g., Berlin, \textit{supra} note 10.

\textsuperscript{16} \textit{AG Muenchen, supra} note 10; see also Mary Lisbeth D'Amico, \textit{Germany Troubled by CompuServe Porn Conviction}, \textit{INDUSTRY STANDARD}, May 29, 1998 [http://www.thestandard.net/articles/news_display/0,1270,439,00.html].

\textsuperscript{17} Strafgesetzbuch [StGB], v. 15.5.1871 (RGBI. S.127), last amended 26.1.1998 (BGBI. I S.1607).

\textsuperscript{18} Gesetz ueber die Verbreitung jugendgefaehrdender Schriften [Law Against the Distribution of Materials Endangering Minors] [GjS], v. 29.4.1961 (BGBl. I S.497), last amended 22.7.1997 (BGBl. I S.1870).

\textsuperscript{19} \textit{AG Muenchen, supra} note 10, at 22-27.
ated by CompuServe Deutschland GmbH. Via the same connection, German customers of CompuServe, Inc. also had access to extremely violent video games that had been rated PG-18 by the competent German agency.\textsuperscript{20} As before, the German subsidiary directed by Mr. Somm only facilitated access by CompuServe, Inc.'s German customers to the materials posted by CompuServe, Inc.'s U.S. customers on CompuServe, Inc.'s servers in the United States. It did this by maintaining a dedicated phone line between the servers in the United States and German Internet gateways.

There is little doubt that the contents in question did indeed qualify as illegal materials under sections 184 StGB and 21 GjS and that the defendant helped distribute them. Without the specific limitations provided by the new German Internet law, which will be discussed in more detail in this Article, a conviction might have been justified. There were, however, according to the first statements of German criminal law scholars on legal questions involving the Internet,\textsuperscript{21} strong arguments for supporting an acquittal as well. Under the new Internet law, Mr. Somm was clearly exempt from criminal liability, which even the District Attorney conceded in the request for an acquittal. The contrary opinion of the Munich court will be described and briefly criticized in the remaining part of this section below. The critique will then be further explained in the following sections of this Article where the applicable German law is discussed in more detail.

The Munich judge found that CompuServe Deutschland GmbH qualified as an Internet Service Provider under section 3 Nr. 1, 5 II TDG of the new federal German Internet law (see Part II.B.3.a.i infra) because it assisted its parent company in providing Internet newsgroup services to German Internet Users.\textsuperscript{22} However, the applicability of the federal TDG to these circumstances is questionable. Arguably, the court should have applied the German State Treaty on Media Services (MDStV) because Internet newsgroups qualify as Media Services, not Tele Services (see Part II.A.3.c.ii infra). This possibility was not even discussed by the court.

More importantly, the German subsidiary only assisted its U.S. parent company in providing access to Users, i.e., in its role as an

\textsuperscript{20} The Bundesprüfstelle zum Schutz vor Jugendgefährdenden Schriften [Federal Censorship Commission for Materials Endangering the Youth] publishes a list of materials that may not be accessible to minors. See § 1 GjS.

\textsuperscript{21} See, e.g., Sieber, supra note 10.

\textsuperscript{22} AG Muenchen, supra note 10, at 45.
Internet Access Provider, and therefore it should not be liable at all according to the new German Internet law (see Part II.B.3.a.ii infra). CompuServe Deutschland GmbH was never involved in the process of enabling the Content Providers of the pornographic newsgroup files to publish their contents on the Internet. This was done via servers in the United States over which the German company had no control. Therefore, the German subsidiary never acted as an Internet Service Provider.

The court, without further analysis, summarily concluded that the German subsidiary had no customers itself and therefore could not qualify as an Access Provider. It reasoned that if CompuServe, Inc. was acting as a Service Provider, and the two companies were to be regarded a single entity since they acted together, then the German subsidiary was also a Service Provider. However, the court's analysis disregards the fact that CompuServe, Inc. also acted as an Access Provider. Accordingly, even if the two companies could be regarded as a single entity, the court should have taken into consideration that CompuServe Deutschland GmbH supported its U.S. parent company only in the role of an Access Provider.

Moreover, even if CompuServe Deutschland GmbH qualified as a Service Provider, it was exempted from criminal liability under the new Internet law. Instead, the court held that the conditions for an exemption from liability for Service Providers under the new rules were not met since the defendant knew of the illegal contents and, according to the court, it was technically possible, reasonable and acceptable for the defendant to prevent further distribution of the illegal materials in question. This last assumption is again very doubtful.

The court conceded that it was, and still is, technically impossible for CompuServe Deutschland GmbH to prevent the distribution of individual contents, such as the newsgroup files in question, since it had and has no control over the servers located and operated in the United States. Therefore, it could not block individual newsgroups. At best, the defendant could have completely shut down the permanent phone line connections between CompuServe, Inc. servers and the German gateways. While this would have ceased the distribution of the illegal contents in question, it also would have blocked all

23. See infra Part II.B.1 for definitions of Access, Content and Service Providers.
24. AG Muenchen, supra note 10, at 44-45.
25. Id. at 47-52.
other contents on the Internet for the German customers of CompuServe, Inc.

As a result, the subsidiary would have gone completely and permanently out of business, which obviously would not be reasonable and acceptable under the new German Internet law (see Part II.B.3.a.i infra). The court’s holding makes no mention of this fact. The court instead focused on a theory of vicarious liability, probably because it realized that it would have been unacceptable for the German subsidiary to completely shut down its business to avoid the transmission of a few offending newsgroup files.

The court argued that the German subsidiary and the U.S. parent company had to be regarded as a single entity for criminal law purposes. Therefore, it was sufficient that it was technically possible, reasonable and acceptable for CompuServe, Inc. to block the individual contents.26 According to general principles of German criminal law,27 a defendant can only be held responsible for his own personal conduct and actions related to a company he controls. No provision of the penal code holds a director of a subsidiary liable for its parent company, which he has no control over whatsoever.28 Therefore, when applying the privileges of the new German Internet law to a German company and its directors, the technical possibilities of its U.S. parent company are generally entirely irrelevant.

The Munich Court did not (and could not) refer to any precedent to justify its contrary opinion. Instead, it relied on one vague remark made by the German Bundesrat during the legislative process, the authority of which is very doubtful.29 The court did not make

26. Id. at 48-52.
29. Bundesdrucksache [Federal Parliament Document] [BT-Drs] 13/7385, 51 No. 4(b) & (c). Federal Statutes are enacted by the Bundestag [Federal Parliament] usually after a draft is proposed by the federal government or parliament members of the majority party. The reasons they give in their proposal are commonly relied upon for interpretation purposes. The Bundesrat [Federal State Chamber] is a federal political body representing the interests of the German state governments in the federal legislative process pursuant to articles 50 and 77 GG. In certain cases, the Bundesrat must consent to federal legislation. In those cases, one might consider the Bundesrat’s remarks for the interpretation of a statute, especially if they are confirmed by the proponent of the draft legislation. In connection with the new German Internet law, however, the consent of the Bundesrat was not required and the federal government did not confirm the Bundesrat’s remark quoted
any further attempts to explain why the director of a wholly owned subsidiary could be responsible for the acts of its parent company. It also did not try to explain how, as an exception to the general rule, the defendant had any control over CompuServe, Inc. In light of the circumstances surrounding the relationship between CompuServe, Inc. and the German subsidiary, it is highly unlikely that he, in fact, did have any control.

C. Extraterritorial Application of National Laws and Its Limits

1. General Statutory Provisions on the Applicability of German Criminal Law

Generally, German law applies only to persons, things and acts within Germany's territorial boundaries. Accordingly, section 3 of the German penal code, StGB, states the general rule that German criminal law only applies to acts committed in Germany.

Sections 4-9 StGB contain a number of exceptions to this general rule. Among other things, these exceptions take into account whether certain acts present a danger to the German State and its government and whether they have been committed by, or against, German citizens abroad. However, these cases are not of specific relevance to the Internet and need not be discussed in further detail here.

A more relevant exception to the general rule is section 6 StGB which provides recourse for certain "crimes against humanity," regardless of where, by whom, or against whom, a crime is committed. Besides genocide, slavery and drug trafficking, the sanctions contained in sections 6 Nr. 6, 184 III, IV StGB also apply to the production and dissemination of child pornography worldwide. Accordingly, the court in Mr. Somm's case without a doubt correctly by the AG Muenchen. See BT-DRS 13/7385, 69-75. Accordingly, its authority for interpreting the statute is doubtful. Moreover, the remark of the Bundesrat on which the AG Muenchen relied hardly supports the court's reasoning. The Bundesrat pointed out that, in his opinion, it might be necessary to hold German divisions of multinational corporations responsible for servers operated abroad, for example, if a dedicated phone line was maintained. The Bundesrat, however, did not further specify or discuss whether its remark referred only to the responsibility of a German parent company for a server operated by its wholly owned and controlled foreign subsidiary, or whether it also applied to situations where the German subsidiary had no control over the server abroad, as in the case before the court.

30. Strafgesetzbuch [StGB], v. 15.5.1871 (RGBI. S.127), last amended 26.1.1998 (BGBl. I S.1607).

31. Imprisonment between 3 months and 5 years or fines.
assumed the applicability of German criminal law provisions to child pornography. Had the Munich District Attorney found and indicted the U.S. management of CompuServe, Inc. or the private U.S. residents that posted the pictures on the newsgroups, the Munich court would have applied German criminal law to them as well.

Apart from the aforementioned exceptions to the general rule (section 3 StGB), section 9 I StGB defines in more detail which acts are deemed to be committed in Germany. Section 9 StGB differentiates between provisions that sanction acts which cause a detrimental effect (e.g., someone’s death or injury) and provisions sanctioning certain conduct (e.g., drunk driving or disseminating illegal materials).

According to section 9 I StGB, provisions relating to conduct generally apply only if such conduct is committed on German territory. With regard to the provisions that sanction acts causing a detrimental effect, however, section 9 StGB defines a different range of international applicability. It is sufficient if an effect is produced or intended to be produced in German territory, and it does not matter where the acts causing the effects are committed. The classic example of the application of this rule, contained in most legal systems worldwide, is the foreigner who, for example, shooting from Austrian territory across the border, kills someone in Germany. Most national legislators feel it is necessary to extend the applicable range of national laws to foreigners outside the national territory to prevent certain detrimental effects within their own territory.

2. International Law Limits on National Jurisdiction to Prescribe

It appears to be generally accepted that the aforementioned German rules regarding conduct abroad producing effects in German territory are in accordance with international customary law, as long as they only address detrimental effects that directly and physically

32. Hilgendorf, supra note 12, at 1873; Barbara Breuer, Anwendbarkeit des deutschen Strafrechts auf extraterritorial handelnde Internet-Benutzer [Applicability of German Criminal Law to Internet Users Acting Extraterritorially], 1998 MMR 141, 142.
34. See SCHACHTER, supra note 8, at 262; OPPENHEIM’S INTERNATIONAL LAW, supra note 8, at 459.
materialize on German territory. Under these circumstances, the application of national laws is justified by the generally accepted international law principle of territorial sovereignty expressed in the theory of "constructive presence" of the perpetrator.

The controversial "effects doctrine" need only be employed in cases where States apply their national laws to extraterritorial conduct causing indirect effects, such as trade between Canada and Cuba, which might adversely affect the financial interests of expropriated U.S. citizens. Apart from the question of whether the effects doctrine in fact constitutes international law and, if so, how extensive or narrow it must be interpreted, it must be asked, whether the effects doctrine is even required to justify the exercise of national legislative powers over conduct occurring abroad. Given the history of numerous controversies in this area, it appears doubtful whether there was ever enough consensus between the nations on this question to create customary law.

3. Concept of Territoriality Imposes Few Significant Limits in Cyberspace

Even if one assumed customary international law restricted not only the national jurisdiction to adjudicate and enforce, but also a State's jurisdiction to prescribe, the criteria traditionally employed to determine whether such restrictions have been exceeded are unsuitable in cyberspace. All of the contents on the Internet can materialize and cause effects anywhere in the world. Thus, the alleged international law rules limiting national jurisdiction to prescribe lose their restricting effects on the Internet.

35. See generally Oppenheim's INTERNATIONAL LAW, supra note 8, at 459.
36. Id.
37. See SCHACHTER, supra note 8, at 261-64; OPPENHEIM'S INTERNATIONAL LAW, supra note 8, at 471-76.
Similarly, the German statutory provisions drafted to restrict the applicability of national laws (e.g., sections 3-9 StGB discussed supra) also lose their rationality when applied to cyberspace cases. This can be illustrated by a hypothetical recently constructed regarding the Internet.

Under section 185 StGB, it is a criminal offense to insult another person, i.e., to say something seriously derogatory to him or about him to a third party. The fact that the insult is made known to a third party is regarded to be a "detrimental" effect under German criminal law. Thus, according to section 9 I StGB, German criminal law applies. If student A in California included insulting opinions on his Internet home page about fellow student B, his next door neighbor, and, coincidentally, German student C viewed this home page on his personal computer in Munich, according to sections 3, 9 I, 185 StGB, student A would have committed a criminal offense in German territory.

It is, however, not very likely that A would ever be charged for his acts in Germany. According to section 194 StGB, a prosecution under section 185 StGB requires a formal application by the insulted person, student B, a requirement which is highly unlikely to be met under such circumstances. Nonetheless, this hypothetical highlights the acute need to discuss the limits of the extraterritorial application of national criminal law in today's globalized information society.

The assertion of jurisdiction on the basis of the effects doctrine or by extensive reference to legal constructions such as constructive presence is practiced predominantly by the United States, the European Community and Germany. It has been the issue of much controversy in the past, and it is predestined to cause conflicts in con-

40. Hilgendorf, supra note 12, at 1876.
42. Hilgendorf, supra note 12, at 1876.
43. Id. at 1874.
44. A recent example is the Helms-Burton Act and the EC Blocking Regulation. See supra text accompanying note 38. For more examples of an "assertion of jurisdiction on the basis of an alleged 'effects' principle of jurisdiction," see OPPÉ-HELM's INTERNATIONAL LAW, supra note 8, at 475; SCHACHTER, supra note 8, at 261-64; OEHLER, supra note 33, at 207-43. According to the Permanent Court of International Justice, international law does not contain "a general prohibition to states to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory." Lotus case, Judgment no. 9, 1927 P.C.I.J. (ser. A) No. 10, at 19-20. See also EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248
nection with the Internet, where most contents can materialize and cause "effects" in every jurisdiction and territory in the world. The goal of international accord and harmonization of national laws will not likely be attained by simply applying a "requirement of reasonableness"45 or waiting for the development of customary international law in an area of rapidly changing information technology. The hope, therefore, lies in the possibility of agreements and treaties.46

It should be noted, though, that the precedents and situations discussed above in Parts A and B and below in D are not even based on circumstances where Germany’s jurisdiction to prescribe, adjudicate and enforce was in fact doubtful. Without the need for employing the controversial effects doctrine, Germany had jurisdiction according to the traditional and generally accepted international law principle of territorial authority. In the Felix Somm case (see Part I.B supra), both the defendant and the illegal contents were physically present in German territory, the latter materializing on a server and personal computers located in Germany. In addition, certain acts were committed in German territory where the contents were transferred via the dedicated line and received by German Users. Although—contrary to the court’s decision—German criminal law did not provide for sanctions against Mr. Somm, the German government, without a doubt, had the jurisdiction to prescribe such sanctions under customary international law.

D. Potential Consequences for Private Users

Private individuals also may be impacted by the laws of other countries, at least indirectly. Depending on the contracts governing Internet access by U.S. Users and Content Providers, it is possible that private individuals with no assets abroad could be substantially affected by the enforcement of foreign laws prohibiting their published content on the Internet. For example, had the Munich court, in addition to convicting its director,47 fined the German subsidiary of CompuServe, Inc. the equivalent of US$50,000, CompuServe, Inc.

(1991) (emphasizing that “Congress has the authority to enforce its laws beyond the territorial boundaries of the United States”); Steele v. Bulova Watch Co., 344 U.S. 280 (1952); Strassheim v. Daily, 221 U.S. 280, 284 (1911).

45. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §§ 402, 403 (1987); Yoo, supra note 39, at 756-57; SCHACHTER, supra note 8, at 258-61.

46. Staiman, supra note 5, at 866.

47. This is possible according to section 30 of the Ordnungswidrigkeitengesetz [Code on Administrative Fines and Offenses].
might have passed those fines onto its customers, the Content Providers who originally published the child pornography on the company's server. This shift of liability can be accomplished by simply including an indemnification clause in the original customer agreement which governs the terms of Internet access. This way, a private individual publishing on the Internet might end up paying a substantial fee which has been imposed by a foreign State with the intent to pressure an international corporation into compliance with that country's local rules.

E. Conclusion

Since content published on the Internet locally can be transferred to any foreign territory at any time, the applicability of foreign law is only a few buttons or mouse clicks away. Due to the complex economic connections and other existing links in today's globalized information society, Internet Users and providers can be affected by the standards imposed by foreign governments, even if they are not their direct addressees. Under these circumstances, while it is impossible for any individual to keep informed about all foreign law restrictions on content placed on the Internet, it might be advisable to be aware of a few basic principles applied in other jurisdictions. Understanding the foreign law is also the first step towards developing realistic concepts that could underlie a uniform international law on Internet censorship or, alternatively, a uniform restriction on the application of national laws to internationally published content.

II. New German Statutes Governing Online Services

The bad news is that instead of one new code, there are more than twenty. The good news is that, nevertheless, nearly the same rules apply for all online services everywhere in Germany because the individual states have enacted uniform codes that resemble the federal law.

These rules are explained and compared to U.S. law in Part II.B infra. First, however, it is necessary to examine the reasons why these different statutes were passed in order to understand the problems regarding their constitutionality and their ranges of applicabil-
ity.

A. Range of Applicability of the Federal Law (IuKDG) and the Uniform State Codes (MDStV) on Internet Services

1. General Federal Rules for All Online Services, Specific Federal Rules for Tele Services and Specific State Rules for Media Services

The federal statute on information and communication services, the Informations- und Kommunikationsdienstegesetz (IuKDG)\(^4\) consists of two new statutes specifically dealing with Tele Services:

- a specific code on Tele Services, the Teledienstegesetz (TDG), and
- a code on data protection in connection with Tele Services, the Teledienstedatenschutzgesetz (TDDSG).

The federal IuKDG contains a third new code that sets up electronic signature rules applicable to all online services, called the Signaturgesetz. In addition, the IuKDG amends certain existing federal statutes, the StGB,\(^5\) the GjS\(^6\) and the intellectual property code (UrhG).\(^7\) As a result, the StGB and UrhG now apply to all online services, i.e., Tele Services and Media Services, whereas most provisions of the GjS apply only to Tele Services.\(^8\)

Rather than passing sixteen different individual codes, the Ger-

\(^{50}\) Strafgesetzbuch [StGB], v. 15.5.1871 (RGBI. S.127), last amended 26.1.1998 (BGBl. I S.1607).

\(^{53}\) The content-based speech restrictions of the GjS have been extended only to Tele Services. Section 7(a) GjS is worded more broadly and requires the appointment of a Youth Protection Officer for all providers of online services, including providers of Media Services. See discussion infra Part II.B.4.b. This extension of the GjS was unsuccessfully critized by the Bundesrat. See BT-Drs 13/7385, 52; see also BT-Drs 13/7385, 70 (federal government answer claiming that a uniform provision on Youth Protection Officer is so important that it must be in the federal code). The practical relevance of the GjS extension to Media Services is little, however, since the exact same requirement is also imposed by state law, and the federal parliament did in fact have the legislative power to comprehensively regulate the subject of youth protection. See § 8 IV MDStV, v. 20.5.1997 (Hessisches GVBl. I S.134, Berliner GVBl. I S.361); art. 74 Nr. 7 GG. But see Schulz, supra note 2, at 183.
man Federal States each passed uniform state laws on Media Services. This uniformity was accomplished by the Treaty on Media Services, the Mediendienststaatsvertrag (MDStV), the provisions of which were passed as a state code in all sixteen federal states. These statutes will collectively be referred to as the MDStV herein. The MDStV contains provisions on the same topics covered by federal law, i.e., the liability of online providers, data protection and protection against violent and pornographic materials. In addition, the MDStV contains traditional media provisions, such as a right to reply.

The reasons for the legislative differentiation between Tele Services and Media Services lie exclusively in the area of legislative powers.

2. State and Federal Legislative Powers in Germany and the Legislative Powers of the European Community

a. Vertical Separation of Powers in Germany

The parameters of state and federal legislative powers within Germany are laid down in the German constitution, the Grundgesetz (GG). According to articles 30, 70 and 83 GG, all administrative, judicial and legislative powers are assigned to the states, unless expressly designated otherwise in the constitution. Federal administrative powers are very limited and only cover a few areas, for example, foreign affairs, aviation, nuclear power and social security. Similarly, judicial powers are mainly exercised by state courts, which decide nearly all cases as courts of first and second instance, regardless of whether federal or state law applies. With few exceptions, federal courts are limited to deciding questions of federal law as courts of last instance. In the area of legislation, however, the German constitution provides for a substantial number of exclusive and concurrent federal legislative powers.

54. See Staatsvertrag ueber Mediendienste [Treaty on Media Services] [MDStV], v. 20.5.1997 (Hessisches GVBI. I S.134, Berliner GVBI. I S.361).
55. See, e.g., Gesetz zu dem Staatsvertrag ueber Mediendienste [Code Implementing the Treaty on Media Services], v. 23.6.1997 (Berliner GVBI. I S.369).
56. Art. 70-75 GG, v. 23.5.1949 (BGBl. I S.1), last amended 20.10.1997 (BGBl. I, 2470); see supra note 27.
57. Id. art. 83-91.
58. Id. art. 95-96.
b. Most Subjects Fall Under Federal Legislative Competence

Among the areas of exclusive federal legislative powers are foreign affairs, telecommunications and intellectual property. The areas of concurrent federal and state jurisdiction include criminal, civil, labor and antitrust law, court procedures, protection of the youth and the law of commerce.

In areas of concurrent federal jurisdiction, the federal parliament may pass statutes if a uniform national law is in the best interest of the country and is necessary in order to achieve comparable standards of living across the country or to preserve the commercial and legal unification of Germany. In the past, the Federal Constitutional Court of Germany, the Bundesverfassungsgericht (BVerfG), has rarely declared statutes unconstitutional for failing to meet this standard. The BVerfG generally defers to the judgment of the federal parliament.

In areas of concurrent jurisdiction, the states may pass laws only if they are in an area not yet legitimately regulated by federal statutes. The federal parliament, however, has used its legislative powers extensively. Therefore, despite the abstract rule of articles 30 and 70 GG, there are, in fact, only a few areas left to state legislation. Traditionally, these areas included regulation of state administrative bodies, police, culture, education, the press, broadcasting and other media.

c. State Law Governing the Press and Other Media

The German federal states are very eager to protect their few

59. Id. art. 73 Nr. 1, 7 & 9.
60. Id. art. 74 Nr. 1, 7, 11, 12 & 16.
61. Id. art. 72 II.
62. The powers and functions of the BVerfG resemble those of the U.S. Supreme Court, however, the BVerfG may only decide issues of constitutional law, e.g., the constitutionality of statutes, court decisions and administrative acts. The BVerfG is not a general appellate court of last instance, and it may not apply and interpret statutory law, other than the constitution. See Christian Pestalozza, Verfassungsprozessrecht [Constitutional Court Procedures] 3-7 (3d ed. 1991).
63. Ingo von Muench & Philip Kung, Grundgesetz [Commentary on the Federal Constitution], art. 72 Nr. 18 (3d ed. 1996). In 1994, the language of the German Federal Constitution was modified to compel the BVerfG to apply stricter standards. Id. Thusfar, however, no changes have become apparent.
remaining areas of legislative powers. During the last ten years, the European Community has constantly threatened the area of culture and media regulation. For example, the German states traditionally owned public television and radio broadcasting stations which are supposedly politically neutral and independent. These stations are financed by fees, imposed by a state code and collected by a public agency. Anyone who owns and uses a radio or television in Germany must pay those fees regardless of whether he watches public broadcasting and cable television or only private channels.

This practice has been justified on the grounds that the mere technical possibility of the receipt of public broadcasting by any radio or television is sufficient so that it cannot be ruled out that someone who claims he is watching only private television may, in fact, be watching public programs. The public stations refuse to broadcast their programs in encoded form which would allow viewers to decide whether they want to pay to see public television. Their purported concern is that the majority of the population would be unduly burdened with the costs of decoders. Even private television broadcasters must pay state fees for the television sets they use to monitor their public competitors, though they themselves do not charge any similar fees.

This system is hardly compatible with the general principles of a free common market in Europe, and it specifically violates article 92 of the Treaty Establishing the European Community (TEC). Even
though the European Union Member States recently expressed support for existing methods of public radio and television financing in a vague declaration accompanying the Amsterdam Treaty, it is very doubtful that German radio fees would survive a lawsuit before the European Court of Justice.

The German state broadcasting system is additionally threatened by the fact that, in the Internet world, the blocking and encoding of individual programs is very common and does not cause undue costs. Moreover, software programs would allow easy verification of whether one had consumed public broadcasting, thereby removing any need for encoding.

Instead of adjusting the antiquated fee system, the state legislators allowed their public broadcasting stations to set up their own online services. The stations then announced plans to charge broadcasting fees for any personal computer that could receive their communications, i.e., any personal computer that is online. In response to an uproar by Internet Users, a three year moratorium was implemented.

Any expansion of the use of legislative powers by the German federal parliament or the European Community in this area would further undermine the ability of the states to defend their system. For that reason, the states decidedly oppose all attempts to facilitate such expansions on bordering subjects such as telecommunications and commerce.

d. Precedents

The German states traditionally argued that television and radio broadcasting are merely cultural and media affairs which do not fall under either the German federal parliament’s or the European Community’s powers to regulate commerce or telecommunications.
This position was first confirmed by the BVerfG when the states challenged the foundation of a federal German television station in 1961. The court held that federal telecommunications jurisdiction only extends to the technical aspects of broadcasting (i.e., assignment of frequencies, etc.) and not to its content.\(^\text{74}\) Therefore, the federal parliament may not pass legislation on the content of broadcasting or set up its own broadcasting station. The principles of the 1961 decision regarding the distribution of legislative powers within Germany have been confirmed by the BVerfG several times since.\(^\text{75}\)

Even though the European Court of Justice has not yet explicitly decided whether European Community legislative powers extend to this area, there is little doubt that the Court would be inclined to answer this question in the affirmative. There are already a number of applicable European Community Directives in the areas of telecommunications\(^\text{76}\) and television broadcasting\(^\text{77}\) which are constantly applied by the European Court of Justice.\(^\text{78}\) In addition, the European Court of Justice has applied the provision on the free movement of services in the TEC\(^\text{79}\) to television transmissions since 1974.\(^\text{80}\) Accordingly, the European Community can claim legislative powers for the coordination of national Member State laws restricting the freedom to provide services under articles 57 II and 66 TEC.

Moreover, the BVerfG explicitly accepted the legal position of the European Court of Justice in a recent decision.\(^\text{81}\) In the underlying case, the German states sued the federal government for approv-
ing the enactment of the European Community Council's European Community Broadcasting Directive. The German states claimed that neither the German federal government nor the European Community had the legislative power to regulate in this area. The BVerfG held that the TEC is paramount, and it assigns the Community the legislative power to regulate television broadcasting as commercial services.82

e. European Community Remained Inactive

Notwithstanding the potential existence of European Community jurisdiction, the European Community Council has not yet reached a consensus on comprehensive, specific online legislation. A proposal to extend the range of applicability of the broadcasting directive83 and its content-based speech restrictions to online services failed in 1996.84 Nevertheless, the European Community Commission recently proposed a new directive to the European Community Parliament and the European Community Council aimed at harmonizing Internet intellectual property law within the Member States of the European Community.85 The official introduction mentioned that the Commission was also currently preparing an European Community Directive regarding liabilities arising from the Internet.86 It is expected that the new German Internet law described in this Article will serve as a model law for the Commission's proposal.87

f. Compromise Under Political Pressure

In 1995, due to the fact that the European Community had not acted to regulate the Internet, both the federal and state parliaments in Germany came under political pressure to pass regulations on the Internet due to growing public concern regarding data protection and

82. Id. at 241. The court, however, expressed reservations with regards to the "Culture Quotas." See also Filipk, supra note 65, at 323.


86. Id. at 7 (reason Nr. 12).

87. Sieber, supra note 2, at 654.
shielding minors from pornography and racist hate speech. This raised the question of who had the legislative power to act in this area.88

The federal government claimed that Internet services most resembled traditional telephone services, and therefore the federal legislative competence for telecommunications applied. Also, since the majority of services were commercial, the federal commerce competence applied. Finally, only the federal parliament was competent to pass special rules on the civil and criminal liability of Access and Service Providers. The German states, however, claimed that the Internet was entirely a cultural affair, that it resembled broadcasting and that the federal telecommunications competence only covered the technical aspects of the Internet, not its contents.

In 1996, the state and the federal governments negotiated a compromise. The German states would regulate services that resembled and might eventually replace traditional broadcasting ("Media Services"). On the other hand, the German federal parliament would regulate online services that supplemented and replaced existing telecommunications and other commercial services, such as banking and retail shopping ("Tele Services").

The result of this compromise, which is discussed in more detail below, raises two major concerns:

- Federal and state legislators were unable to define a practicable method of differentiation between Tele Services and Media Services; thus, the scope of the federal IuKDГ and the MDStV of the states remain unclear (see Part II.A.3 infra); and

- Since, under the agreement, the states regulate all aspects of Media Services, including criminal and civil liability, it is possible that the state law violates provisions of Germany's federal constitution, the GG, that provide for federal legislative competence for those areas. These constitutional provisions cannot be suspended by negotiations and compromises (see Part II.B.3.b infra).

---

88. Engel-Flechsig, supra note 2, at 231; MULTIMEDIA, supra note 2, at 7.
3. Statutory Definitions of Broadcasting, Media Services and Tele Services

a. German Federal Statutes Apply Not Only to Interstate and Foreign Communication

The U.S. concept of federal statutes applying to interstate and foreign matters only,9 while the same matters may be concurrently regulated by state law in intrastate situations, is a phenomenon unknown to German law. Unlike article 1, section 8 of the U.S. Constitution, article 74 I Nr. 11 GG assigns the legislative power to regulate commerce to the federal parliament without limitation to interstate or foreign commerce. Accordingly, both the federal IuKDG and the state MDStV apply in each of the sixteen German states. Which set of rules applies to an individual online service depends on whether it qualifies as a “Tele Service,” as defined by section 2 TDG of the federal IuKDG, or as a “Media Service,” as defined by section 2 of the state MDStV. If the states had passed different individual statutes instead of agreeing on a mutual approach in a treaty, each state code would only apply in the respective state.

b. Few Technical Differences Between the Legal Categories

Distinguishing between Tele Services, Media Services and broadcasting can be difficult since the technology covered by the IuKDG, MDStV and state broadcasting law are already very similar from a technical perspective. They will likely merge further in the near future once phone and television cables and satellites are completely linked together.

c. Vague and Similar Legal Definitions

In addition to the confusion arising from technical similarities, the legal definitions of Tele Services, Media Services and broadcasting contained in the first paragraphs of section 2 in each statute are extremely vague. To make matters worse, not only do the examples given by the legislatures in the second paragraphs of section 2 TDG

---

90. The treaty on broadcasting between the German States is called “Staatsvertrag ueber den Rundfunk im vereinten Deutschland” (RStV). See RING, supra note 66. It lays down general principles applicable in all sixteen states. Id. In addition to those principles, the states passed individual codes with more detailed rules on public and private broadcasting which apply only in each respective state. Id.
and MDStV fail to clarify these definitions, they actually overlap.\footnote{The definitions are contained in section 2 I Teledienstegesetz [Tele Services Statutes] (see supra Part II.A.1), section 2 I MDStV, v. 20.5.1997 (Hessisches GVBl. I S.134, Berliner GVBl. I S.361) and section 2 II RStV, cited in RING, see supra note 66, at C-0 StV. The examples are contained in section 2 II TDG and section 2 II MDStV.}

i. Tele Services

Tele Services are defined in section 2 I TDG as “electronic information and communication services based on transmissions via telecommunications devices, intended for individual use of visual and acoustic data.” According to the legislative history, the TDG was apparently intended to cover mainly commercial services, offering one-to-one communications and services based on individual requests, in contrast to services that are disseminated to the public like broadcasting or cable television.\footnote{MULTIMEDIA, supra note 2.}

Section 2 III TDG, however, states that non-commercial services can also qualify as Tele Services. Section 2 II TDG gives examples of Tele Services, including tele-banking; information services such as traffic, weather and stock exchange information; commercial advertising for goods and services; services to facilitate the use of the Internet and other nets;\footnote{Search engines are an example.} video games; and offerings of goods and services with the direct option to order electronically, all available on request. The official reasons accompanying the government draft of section 2 TDG further name as examples of Tele Services a discussion forum, tele-commuting, tele-medicine, tele-learning, home pages, search engines, mail order businesses, broker services and consulting services.\footnote{BT-DRs 13/7385, 18-19.}

Especially with respect to home pages and discussion forums such as newsgroups, however, some services are primarily edited for influencing public opinion and therefore qualify as Media Services according to sections 2 II No. 2, III No. 3 TDG and 2 MDStV. Therefore, it is difficult to understand why the court, in its decision against Mr. Somm (see Part I.A supra), applied federal law without any discussion or giving any reasons for its definitional choice.

ii. Media Services

Media Services are defined in section 2 I MDStV as “visual and
acoustic, electronic information and communication services transmitted via electromagnetic waves, addressed to the public.” The MDStV was intended to cover both communications aimed at or capable of influencing public opinion as well as any online services resembling classic television and radio, i.e., disseminated services in contrast to services that are only available by individual request. 95 Section 2 II MDStV gives examples of Media Services, including offerings of goods and services to the public, if they are disseminated (e.g. television shopping); disseminated information services; and all online services available on request, except for video games and services facilitating one-to-one exchanges of goods and payments or the mere transfer of data. Since, for example, home pages and newsgroups do not necessarily fall in these excepted categories, they can also qualify as Media Services. 96

iii. Broadcasting and Cable Television

Finally, Broadcasting is defined in section 2 I RStV as “visual and acoustic performances transmitted to the public via electromagnetic waves.” Supposedly this refers only to traditional radio and television, i.e., diverse programs that include television shows, news and movies as well as specialty channels. 97

iv. Critique

The impracticability of differentiating between Tele Services, Media Services and broadcasting by employing these definitions is obvious and has already been heavily criticized by German scholars in their first reviews of the new codes. 98 However, compliance may not be impossible since the requirements of the TDG and MDStV provisions are markedly similar on the majority of practical issues. Providers who are uncertain which statute applies to their services 99

95. See MULTIMEDIA, supra note 2.
97. RICKER & SCHIWY, supra note 68, at 61-82.
98. Gounalakis, supra note 2, at 2994-95; Kroeger & Moos, supra note 2, at 462; Pichler, supra note 2, at 80; Rossnagel, supra note 2, at 2-3; Waldenberger, supra note 2, at 124. Government officials attempt to defend the statutory definitions by pointing to the problems arising from the disappearance of traditional distinctive marks, such as mass communication versus individual one to one communications, in the field of new media. See Engel-Flechsig, supra note 2, at 238; von Heyl, supra note 2, at 115.
99. Another question is whether “service” refers to single WWW pages or the complete offer of a certain Content Provider. The only practical interpretation
B. Rules of the New German Multimedia Law

The new statutory provisions lay down a number of different requirements and specific rules for the activities of the different players on the Internet. This section will first discuss the different categories of “players,” and then provide an overview of the rules.

I. Providers and Users

Simply put, the roles of the players in the Internet can be divided into five categories: Content Providers, Access Providers and Service Providers (collectively referred to as online providers), Telecommunications Carriers and Users. Their Internet functions are depicted both in the chart and the textual description on the next page.

---

seems to be to view all content available on one Internet address as one “service” under the MDStV and the IuKDg. See Waldenberger, supra note 2, at 125.

100. See Ring, supra note 66 (§ 20 II RStV); Verwaltungsgericht Stuttgart [Local Administrative Court], 1998 MMR 322, 324.

101. The new German Internet law categorizes the different cyberspace players into Content Providers, Access Providers, Service Providers and Users. As these terms are currently neither terms of the industry nor commonly or uniformly used expressions, they appear capitalized throughout this article.
Content Providers and Users are the cyberspace equivalents of traditional speakers and audience. The Content Provider selects and publishes information which is made available to the User. It uses the computer (server), online connections and software of a Service Provider to publish this information on the Internet. The Access Provider grants Users access to the Internet and often provides software, online connections and e-mail accounts on its server. That way, the User can receive and access contents disseminated via, or published on, the Internet. The telecommunications lines that link all servers together and connect the computers of the Content Providers and Users to the Internet are provided and maintained by Telecommunications Carriers, i.e., phone companies and television cable operators.

In this role, Telecommunications Carriers fulfill similar functions as in their traditional telephone business, and it is not apparent why the rules regarding their liability and responsibility require modification. Currently, as the carriers are usually unable to execute any control over the contents transmitted, they normally are neither liable nor responsible for their customers' communications. There is also no apparent reason why Content Providers and Users should be treated differently from offline speakers and audiences. It is questionable, however, to what extent, if any, classic media roles such as editors, news agents or phone companies are comparable to Access and Service Providers. For purposes of clarification, both the CDA and the new German Internet law provide specific rules in this area (see Part II.B.2 infra).


103. See Telecommunications Act of 1996, section 509, 47 U.S.C. section 230 (e)(3) (1996), for the legal definition of "Information Content Provider." But see Waldenberger, supra note 2, at 124 (commenting that users publishing a home page do not qualify as Content Providers because home pages do not constitute a service).

104. Ruth Hill Bro, Defamation Online, in ONLINE LAW, supra note 48, at 335, 342-44.

Many individuals and companies that are active in cyberspace will, from time to time, perform more than one of these roles. For instance, phone company X (i.e., a telecommunications carrier) might provide Internet access to Content Providers and therefore be a Service Provider. In most cases, company X would also then choose to provide access to Users, and in that function, qualify as an Access Provider. For marketing purposes, company X will most likely have a home page, making it a Content Provider as well. When company X searches the Internet for information on its potential customers and competitors, it becomes a User. Thus, the responsibility and potential liability of company X for the publication or transmission of an individual piece of information will depend on the role that company X played in that specific context.

In Mr. Somm's case (see Part I.B supra), U.S. customers of CompuServe, Inc. posted materials on CompuServe, Inc.'s servers. In this role, CompuServe, Inc. acted as a Service Provider with its customers as Content Providers. CompuServe Deutschland GmbH was not involved at all in this relationship and, therefore, does not qualify as a Service Provider. However, CompuServe, Inc. also made the materials posted by its U.S. customers available to German Internet Users. In this context, CompuServe, Inc. acted as an Access Provider. CompuServe Deutschland GmbH supported CompuServe, Inc. as an Access Provider by providing technical support and maintaining a dedicated phone line. Therefore, CompuServe Deutschland GmbH qualified only as an Access Provider, contrary to the opinion of the court.

2. Specific Content-Based Speech Restrictions on the Internet and Defenses

The constitutional principles of the protection of free speech in the United States and in Germany are somewhat different.106 Obscene speech, fighting words and speech presenting a clear and present danger are excluded from protection by the First Amendment in the United States.107 These types of speech, however, are protected in

107. JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW 986-1041
Germany under article 5 I GG, which extends protection to all speech except intentional lies. Article 5 I 3 GG specifically bans censorship, which is generally interpreted to prohibit only prior restraint. On the other hand, article 5 II GG explicitly imposes a duty on the German legislature to protect individuals' personal honor and the youth against the dangers associated with free speech. Accordingly, the federal and state parliaments have thoroughly restricted the dissemination of obscene, violent, racist and defamatory materials.

Thus, the new German Internet law had to meet somewhat different constitutional standards than the CDA. For the reasons outlined below, the IuKDG and the MDStV, in contrast to the CDA, do not raise any freedom of speech concerns.

a. No New Content-Based Speech Restrictions in the New German Federal Internet Law

Similar to the situation in the United States, some general criminal law provisions of the StGB prohibited the distribution of illegal contents, such as child pornography, long before the Internet became a matter of public interest.

i. Extension of Existing Speech Restrictions

The new federal Internet law does not prohibit any categories of speech or expression on the Internet that are legal in other forms and media. The IuKDG only adds “computer data, images and sound in electronic, downloaded form” to the examples of the legal definition


109. German statutes generally do not refer to “indecent” communication. The swear words at issue in the U.S. Supreme Court decision FCC v. Pacifica Foundation, 438 U.S. 726, (1978), would not have been an issue in Germany.


112. See § 184 III StGB.

113. Id. § 184 III, IV.
of "document" in existing statutes such as the StGB, the GjS and the UrhG. That way, all existing provisions regarding unlawful documents, including pornographic documents, excessively violent documents and documents violating intellectual property laws, now apply to data downloaded on servers and computers as well. Real time transfers such as live broadcast transmissions of cultural or sports events or interviews are still not covered.

ii. Specifically: Racist Hate Speech

Although not new, one noteworthy difference between German and U.S. law is that document publication, distribution and subscription (including electronic messages), containing or promoting Nazi propaganda and other racist hate speech, is a criminal offense under section 130 StGB, a provision which is strictly enforced. Similar rules exist in other European countries, like France.

iii. Obscenity

As outlined above, the existing GjS was amended to apply to Tele Services. According to this code, it is a criminal offense to make certain obscene, violent or racist contents available to persons under eighteen years of age. Communications between parents and their children are exempted in order to protect parental discretion as protected by article 6 GG. Federal law withholds liability for the con-
tents of Tele Services as long as it is technically possible for Users to prevent access of minors to harmful contents.\textsuperscript{122} The technical means or devices used to prevent access do not have to be provided by the online provider distributing the pornographic content. It is sufficient that the technical means exist so that, for example, parents can offer “safe” usage of the Internet to their children by installing devices such as “Cyberpolice” or “Adult Check.”\textsuperscript{123} In sum, federal law allows the distribution of adult communications if generally available technology allows parents to prevent their children from accessing such contents.

\textit{b. References to Federal Law in the State Code}

The MDStV does contain content-based restrictions specifically applying to Internet communications. The respective provisions do not, however, prohibit content that is unrestricted outside the Internet. They merely repeat and refer to existing content-based speech restrictions in federal statutes. It is very doubtful that the legislative power of the states permits enacting such provisions. As outlined above, in the area of concurrent legislative powers, the states may not pass codes on subjects already regulated by federal codes. The practical relevance of this problem is, however, very limited. Since the sanctions imposed by the StGB are more severe than any state law, state district attorneys apply those provisions over weaker state regulations. Under the federal constitution, a person cannot be sanctioned on the basis of federal and state law twice for the same act. As a consequence, only the federal law is usually applied.

In the area of material endangering the youth, contents in Media Services are governed exclusively by the MDStV, not the GjS. The provisions of the MDStV cover basically the same materials in Media Services as the federal GjS does with respect to Tele Services. The MDStV, however, does not impose prison sentences but only fines. The defenses of the MDStV also differ slightly from those available under federal law.

With regard to contents which were made available to Users at their express request, similar to the federal GjS provisions, the MDStV withholds liability as long as it is technically possible for Users to prevent access of minors to harmful contents.\textsuperscript{124} For contents

\begin{itemize}
\item \textsuperscript{122} § 3 II 3 GjS; Art. 6 Nr. 3 IuKDG, v. 22.7.1997 (BGBI. I S.1870-1879).
\item \textsuperscript{123} See Schulz, supra note 2, at 185-87.
\item \textsuperscript{124} § 8 III MDStV, v. 20.5.1997 (Hessisches GVBl. I S.134, Berliner GVBl. I
\end{itemize}
that are disseminated without specific requests, providers who make materials generally available to the public must take active steps to ensure that minors will not be able to gain access to these types of materials. Under state law, late night transmission is listed as a sufficient precaution.\textsuperscript{125}

c. \textit{Speech Restrictions in the United States: The CDA}

The U.S.'s CDA\textsuperscript{126} contains a number of content-based restrictions on the freedom of speech in interstate or foreign communications via telecommunications devices.

i. Indecent Speech and the First Amendment of the U.S. Constitution

Restrictions on "indecent" communication similar to the ones in 47 U.S.C. sections 223(a)(1)(B) and 223(d) have already caused controversy in the past.\textsuperscript{127} In 1974, the U.S. Supreme Court in \textit{Hamling v. United States}\textsuperscript{128} deemed it necessary to read the prohibition of "every obscene, lewd, lascivious, indecent, filthy or vile article..." as contained in 18 U.S.C. section 1461 to refer only to "obnoxiously debasing portrayals of sex," i.e., only to obscene speech as defined in \textit{Miller v. California}.\textsuperscript{129} Subsequently, the Court implied that the broad wording of the statute prohibiting the sending of indecent mail was unconstitutional under the First Amendment.\textsuperscript{130}

Then, in the 1978 case of \textit{FCC v. Pacifica Foundation},\textsuperscript{131} the U.S. Supreme Court upheld a declaratory order issued by the Federal Communications Commission (FCC) holding that indecent speech in a radio transmission in the early afternoon could result in administrative sanctions based on 18 U.S.C section 1464. The Court reasoned that such content-based regulation was acceptable given the low standard of constitutional protection that generally applied to speech

\textsuperscript{125} Id. § 8 II.  \\
\textsuperscript{127} See Jerry Berman & Daniel J. Weitzner, \textit{Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media}, 104 YALE L.J. 1619, 1629-32 (1995).  \\
\textsuperscript{128} Hamling v. United States, 418 U.S. 87, 112 (1974).  \\
\textsuperscript{129} Miller v. California, 413 U.S. 15 (1973); \textit{William B. Lockart et al., Constitutional Rights and Liberties} 471 (7th ed. 1991).  \\
\textsuperscript{130} This interpretation of \textit{Hamling v. United States} is given by the U.S. Supreme Court in \textit{FCC v. Pacifica Foundation}, 438 U.S. 726, 740 (1978).  \\
\textsuperscript{131} FCC v. Pacific Found., 438 U.S. at 726.
in the broadcasting media since Red Lion Broadcasting v. FCC.\textsuperscript{132} This is because broadcasting "established a uniquely pervasive presence in the lives of all Americans," and since it intruded into the privacy of people's homes, it was "uniquely accessible to children."\textsuperscript{133} Similar statutory restrictions on telephone services in 47 U.S.C. section 223 were found to be unconstitutionally vague and overbroad in Sable Communications v. FCC absent the unique circumstances found to exist in the context of broadcasting.\textsuperscript{134}

Since the unique circumstances of broadcasting are not present in the Internet either,\textsuperscript{135} the U.S. Supreme Court also declared the respective CDA restrictions on indecent Internet communication to be unconstitutionally vague and overbroad in 1997.\textsuperscript{136} In particular, the Court opined that the CDA unduly restricted communications between parents and their children, and the defenses under the CDA were commercially impracticable for non-profit online providers.\textsuperscript{137}

\begin{itemize}
\item \textbf{ii. Extraterritorial Application of the CDA}
\end{itemize}

In Shea v. Reno,\textsuperscript{138} the U.S. District Court for the Southern District of New York assumed, without further explanation or discussion, that "the CDA only regulates content providers within the United States." The Supreme Court regards "the intended, as well as the permissible scope of, extraterritorial application of the CDA" as "difficult issues," but no decision was reached as those issues were held to be not before the court.\textsuperscript{139}

The language of 47 U.S.C. section 223 specifically covers "foreign communication" and therefore undoubtedly applies to Content Providers residing in the United States who send or make available contents abroad. The question is, does the CDA also apply to Content Providers residing abroad who send contents to the United States or even to communications which are entirely carried out be-

\vspace{1cm}

\begin{itemize}
\item \textsuperscript{133} FCC v. Pacifica Found., 438 U.S. at 748-49; see also Berman & Weitzner, supra note 127, at 1630-32.
\item \textsuperscript{134} 492 U.S. 115.
\item \textsuperscript{135} Berman & Weitzner, supra note 127, at 1619.
\item \textsuperscript{136} Reno v. ACLU, 117 S. Ct. 2329 (1997).
\item \textsuperscript{137} Id. at 2348.
\item \textsuperscript{139} Reno v. ACLU, 117 S. Ct. at 2347-48 n.45.
\end{itemize}
The term "communication" generally refers to interactive conduct: speech, listening and answers, i.e., when one writes, reads and responds. Thus, the term communication necessarily also covers conduct abroad in a situation where the speaker and his audience are residing in two different territories. The wording of the CDA could even be interpreted to apply to all communications on the Internet worldwide.

With respect to the applicability of U.S. legislation to conduct abroad, the U.S. Supreme Court generally assumes "that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States."\(^{140}\) The Court further assumes that the legislature is aware of the need to make a clear statement that a statute applies overseas, and opines that the use of the nondescript term "foreign commerce" is not clear enough to express Congress' intent to prescribe extraterritorial application.\(^{142}\)

Under that reasoning, one may conclude that the use of the term "foreign communication" in the CDA is not clear enough to justify its application to communications carried out entirely between foreigners residing abroad. A stronger case could be made, however, that its application to foreign Content Providers sending contents to Users located in the United States, e.g., via e-mail, or even that its application to foreign Content Providers, who intentionally make contents specifically available to Users located in the United States (e.g., by directly addressing them), would not exceed the territorial jurisdiction of the United States. In both cases, the contents do in fact materialize in U.S. territory, namely on servers and personal computers physically located in the United States.

This situation should be distinguished from cases where a User in the United States accesses and brings illegal contents into the United States, which are made generally available worldwide by on-

---

140. A different question is, under what circumstances a U.S. court would have jurisdiction over foreigners residing abroad who potentially violate the CDA and with regard to whom there exist practical possibilities for enforcement. The CDA does not explicitly address this question. It would, therefore, have to be answered by applying general rules of U.S. national law and thus will not be discussed further in this article. The U.S. Supreme Court regards the absence of "any mechanisms for overseas enforcement" as support for employing a narrow interpretation of national laws for their scope of application. See EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 256 (1991).


line providers located abroad. In such cases there is no specific intent or act directly aimed at this result by the foreigner. In such cases, the Content Provider commits the conduct prohibited by the CDA exclusively outside U.S. territory, i.e., outside the territorial jurisdiction of the United States. Therefore, in the absence of an indication by congress, the CDA should not apply under these circumstances to the foreign Content Provider residing and acting abroad.

In the case of a foreign Content Provider who actively sends contents to the United States, however, the prohibited conduct is intended and aimed at reaching into the territorial jurisdiction of the United States. As far as questions of territorial jurisdiction to prescribe are concerned, this situation is comparable to the aforementioned classic hypothetical of someone firing his gun across the Canadian or Mexican border to shoot a U.S. citizen on U.S. ground. Moreover, the analysis is very similar to sending traditional mail. U.S. courts have upheld prosecutions of foreign residents who send fraudulent mail to the United States under respective statutes which are similarly worded to the CDA. Therefore, it appears that the CDA would apply to all Content Providers worldwide who, regardless of their citizenship and residence, actively send messages to addressees in the United States.

d. Conclusion and Comparison

In contrast to the CDA, the new German Internet law does not prohibit any online speech which would be legal offline. The German codes merely extend the applicability of existing speech restrictions to Internet communication. Obscene communication between parents and their children is mostly exempted from criminal prosecution to protect parental discretion. Even those who wish to publish regulated content may do so as long as devices or other means exist which enable the Users to block materials that are considered harmful to the youth. Content Providers do not have to take any specific pre-

cautions themselves as long as these protective mechanisms are generally available. As a result, non-commercial providers are not unduly burdened. Thus, the German codes do not invoke comparable freedom of speech issues as those arising from the CDA. The CDA seems to raise similar uncertainties regarding its extraterritorial application as do the content-based speech restrictions of the German law.

3. Specific Privileges for Access and Service Providers Regarding Secondary Liability

The legislatures of most countries fight the harms and dangers of speech directly by holding the creator of certain materials liable, often by the imposition of criminal penalties.¹⁴⁴ Similar results can also be reached indirectly by regulating the publication, transmission and distribution of speech and other forms of expression. The statutes and case law on "classic" media issues show a very differentiated approach to the liability imposed on the various parties to a particular communication, depending upon their status as authors, editors, publishers or wholesale and retail distributors of newspapers or videos.¹⁴⁵ Before the enactment of specific rules in the United States and Germany, it was heavily debated which of these roles, if any, should apply to Access and Service Providers.¹⁴⁶ Like the CDA, the new Ger-

¹⁴⁴ Defeis, supra note 118, at 57.
¹⁴⁵ Bro, supra note 104, at 342-44; Thomas J. Smedinghoff, Liability for Conduct of Others, in ONLINE LAW, supra note 48, at 461, 469-72.
¹⁴⁶ With regard to U.S. law, see Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31663/94, 1995 WL 805178, at *10 (N.Y. Sup. Ct. Dec. 11, 1995), 24 Media L. Rep. 1126 (N.Y. Sup. Ct. 1995); Johnson, supra note 105, at 589. With regard to German law, see Sieber, supra note 10, at 429. Before the new German multimedia law was enacted, the Amtsgericht Berlin-Tiergarten [Criminal Court of First Instance in Berlin] decided a case where a German politician who was a member of the Socialist Party (legal successor of the former East German government party, the Uniform Socialist Party of Germany) had provided a hyperlink on her homepage leading to a server operated in the Netherlands making an electronic version of a newspaper called "RADIKAL" available. Allegedly after the link was installed, the newspaper published an article approving a terrorist attack on the renowned labor law professor Klaus Adomeit in Berlin as well as information on how to sabotage the German railway. See the statement of the German federal government answering an information request of the Green Party, BT-DRS 13/8153. The Berlin judge held that a Content Provider installing a WWW-hyperlink is responsible only if she knows the contents of the homepage to which the link leads. AG Berlin, 260 -DS 857/96 (June 30, 1997), 1998 CR 111. Since the prosecution could neither prove that the link was installed before the illegal content was published nor that the defendant had actual knowledge of the article, she was acquitted. See id.
man multimedia law contains specific provisions on this subject.

a. Liability of Providers According to Federal Law

As applied to Tele Services, section 5 TDG of the federal IuKDG limits the liability of Service and Access Providers for the transmission of illegal contents on the Internet.

i. Service Providers

According to section 5 II TDG, a Service Provider is only liable for illegal contents which he channels onto the Internet if: (1) he is aware of the substance of the communication; and (2) if it is possible and acceptable for the Service Provider to prevent the publication/distribution of the unlawful contents on the Internet.

The statute does not further specify the term "acceptable." This term appears in many other German statutes, however, and it is generally interpreted to necessitate a balancing of conflicting interests. When proposing the draft of the IuKDG, which was later enacted without any significant changes by the federal parliament, the government explicitly suggested such an interpretation of the term "acceptable" with regard to section 5 TDG. According to the government, the balancing decision should consider the relevance of the incident, the costs of blocking a single file and the impact for other parts of an online service. As an example of a situation in which blocking would not be acceptable to a Service Provider, the government specifically refers to the case of a Service Provider who makes several newsgroups available and is asked to block an entire newsgroup because of illegal contents in a few individual files posted there.

Thus, in Mr. Somm's case (see Part I.B supra), arguably German federal law did not mandate that CompuServe, Inc. block the illegal contents. To block entire newsgroups because of a few files violating German criminal law would have impacted a high number of legal communications and impaired CompuServe's business. Blocking was therefore not acceptable to CompuServe, Inc.

147. It is not necessary that he realizes that the contents are in fact illegal. Pichler, supra note 2, at 87-88; AG Muenchen, supra note 10, at 47.
148. See BT-Drs 13/7385, 20.
149. See supra note 29 for information on the legislative process according to the federal constitution.
150. BT-Drs 13/7385, 20.
151. Id.
Given the extremely negative effects of child pornography and the relatively minor expenses for blocking, however, one might also come to the contrary conclusion with regard to CompuServe, Inc. Even if section 5 II TDG was applicable, these arguments could not be applied to the German subsidiary. Since CompuServe Deutschland GmbH did not make contents available on its own servers, it does not qualify as a Service Provider under section 5 II TDG. Even if it did, it clearly would not have been acceptable for CompuServe Deutschland GmbH to block the controversial newsgroups because the only way to achieve this result would be to entirely shut down the dedicated phone line. This would mean going out of business altogether.

ii. Access Providers

According to section 5 III TDG, an Access Provider is generally not liable for the contents to which he provides access. Under section 5 IV TDG, however, an Access Provider can be ordered by a court or a government agency to prevent the distribution of certain contents to Users if: (1) it is possible and commercially reasonable to do so; and (2) if the agency is unable to directly sanction either the responsible Content or Service Provider (e.g., because they live abroad).

It is controversial whether, according to section 5 III, IV TDG, an Access Provider would be liable even if he had knowledge of the contents he made available. The legislature answered this question in the negative. Otherwise, the differentiation between Access Providers and Service Providers in section 5 II and section 5 III TDG would have been unnecessary.\footnote{152} Accordingly, in the case described under Part I.B, CompuServe Deutschland GmbH and its director, Mr. Somm, should have been exempted from criminal liability.

The German Federal Attorney General, however, did not follow this argument and instead assumed that Access Providers are liable when they knowingly make illegal contents available.\footnote{153} Under that assumption, the Access Provider would be treated similar to a Service Provider. However, even if that view could be followed, Mr. Somm still should have been exempted from criminal liability according to section 5 II TDG since blocking was not a reasonable or acceptable

\footnote{152} Thomas Hoeren, Anmerkung [Case Note], 1998 MMR 97-98.

\footnote{153} See the German Federal Attorney General's formal reasons for terminating criminal proceedings against an Access Provider in the decision of November 26, 1997, 2 BJS104/96-4, 1998 MMR 93-98. This view is heavily criticized by Hoeren, supra note 152, at 97-98.
solution in that case (see Part II.B.3.a.i supra).

If an Access Provider selects a certain content, for example, by installing a hyperlink on his home page, which leads to the home page of someone else, he can qualify as an additional, secondary Content Provider of that home page and be fully liable for its contents. This would be the case if he demonstrated actual knowledge and approval of that home page in connection with the hyperlink, for example, by placing the hyperlink after statements like, “If you want to see more child pornography, go to the home page of X [hyperlink]” or, “As already convincingly argued by A [hyperlink], the XYZ-company is committing fraud on a regular basis.”

However, cases where hyperlinks are provided merely to facilitate access to an anonymous number of contents, for example, in connection with a search engine, have to be treated differently. In those cases, the provider of a hyperlink only qualifies as an Access Provider and is not liable under section 5 III TDG.

iii. Scope of Applicability

The limitations discussed above under subsections i and ii apply regardless of the statutory source of such liability. Thus, Access and Service Providers of Tele Services are exempt from liabilities arising from violations of any German civil, unfair competition, intellectual property, criminal law or other federal or state law committed by Content Providers publishing illegal Tele Services, unless the Access and Service Providers are responsible under section 5 II, III TDG.

154. Flechsig & Gabel, supra note 2, at 354-58.
155. Christian Pelz, Die strafrechtliche Verantwortlichkeit von Internet-Providern [Criminal Liability of Online Providers], 1997 ZUM 530, 532-33. But see Flechsig & Gabel, supra note 2, at 354 (always liable); Waldenberger, supra note 2, at 128-29 (neither §§ 5 I nor §§ 5 III TDG/MDStV apply).
156. The court in AG Muenchen, supra note 10, also generally shared this view. Although it is not yet entirely clear whether all German courts agree with this analysis, it has been supported both by German authors listed below and the German federal government’s answer to an information request of the Green Party before the federal parliament had enacted the IuKD, BT-DRs 13/8153, 8-11. The official reasons accompanying the government’s draft of the IuKD, which was enacted by the parliament nearly unchanged, are less clear but indicate the same understanding. BT-DRs 13/7385, 19-21. See also Sieber, supra note 2, at 583; MULTIMEDIA supra note 2, at 15-17; Rossnagel, supra note 2, at 3; Koch, supra note 2, at 198-203. The Oberlandesgericht Muenchen [Appellate Civil Law Court in Munich] recently applied the German Unfair Competition Law (§§ 1, 3 des Gesetzes über den unlauteren Wettbewerb [UWG], v. 13.8.1997 (BGBl. I S.2038), to an Internet homepage without any discussion of the applicability of the new German Internet law. Section 5 II TDG, however, did in fact apply, although its application would not have
As far as the extraterritorial application of German laws creating liability, section 5 TDG also applies to providers located abroad.\^{157} Therefore, it also applied to CompuServe, Inc. in Mr. Somm's case (see Part I.B supra).

\textit{b. Liability of Providers According to State Law}

Section 5 MDStV provides the same exemptions for Access and Service Providers of Media Services as section 5 TDG does with respect to Tele Services. The validity of section 5 MDStV is, however, doubtful given that the federal constitution assigns the right to enact statutes in the areas of civil, unfair competition, intellectual property and criminal law to the federal parliament, which has, in fact, enacted rules in these areas. According to the principles of concurrent legislative powers, the states may not restrict the applicability of federal codes through state codes.\^{158}

In the past, the BVerfG has accepted provisions in state codes on newspaper publishing which restricted or amended federal statutes on general civil or penal law only if those restrictions historically applied to traditional press law.\^{159} State provisions that did not have such a tradition were held to be unconstitutional violations of the rules on the distribution of legislative powers and therefore declared void.\^{160} Since there is no historical preemption in the area of regulating contents on the Internet, section 5 MDStV is unconstitutional because the states generally do not have the legislative power to restrict the applicability of federal statutes.

Should German courts hold section 5 MDStV void, however, they should apply section 5 TDG by way of analogy to Media Services since section 5 TDG and the compromise reached in its legislative history show that the federal parliament wanted all online services to be privileged.\^{161} Therefore, the same privileges which apply to providers of Tele Services should also apply to providers of Media Services, regardless of whether section 5 MDStV is in fact constitutional. Accordingly, in Mr. Somm's case, it does not matter whether

\begin{footnotes}
\footnote{changed the outcome of the case. See the decision dated February 26, 1998, 29 U 446/97, 1998 CR 300, 300-01; see also Ralf Hackbarth, Case Note, 1998 CR 300, 300-03.}
\footnote{157. BT-Drs 13/8153, 8-9.}
\footnote{158. See infra Part II.A.2; see also Gounalakis, supra note 2, at 2994-95; Koch, supra note 2, at 198.}
\footnote{159. See, e.g., BVerfG, BVerfGE, 7 (1957), 29.}
\footnote{160. See, e.g., BVerfGE, 36 (1973), 193.}
\footnote{161. MULTIMEDIA, supra note 2, at 17.}
\end{footnotes}
the court should have applied section 5 MDStV or section 5 TDG.

c. Liability of Providers According to the CDA

According to section 509 of the CDA, no Access Provider, Service Provider or User shall be treated as the publisher or speaker of any information provided by another Content Provider. According to general principles of U.S. tort law, distributors of information other than the publisher are liable only if the harm created by distribution is brought to their attention.\(^{162}\) Thus, so far, the CDA provision resembles the German section 5 TDG and section 5 MDStV. However, 47 U.S.C. section 230(d) makes it clear that those privileges do not apply in connection with any criminal law, intellectual property law or privacy law. Section 230(d) of the CDA does not even restrict the liabilities arising from section 223. Section 223(e) only rules out any liability of Access Providers under sections 223(a) through (d).

Therefore, had an U.S. action been brought against CompuServe, Inc. under the facts reported above in Part I.B, CompuServe, Inc. would have been fully liable because it was not exempted from any liability under the CDA.

d. Conclusion and Comparison

The new German Internet law contains generous privileges for Access and Service Providers with regard to secondary liabilities. According to sections 5 TDG and 5 MDStV, Service Providers are not liable for distributing illegal contents produced by other Content Providers under any criminal, civil, unfair competition or intellectual property law if they do not know of the illegal contents. In order to avoid liability, they are well advised, in general, not to examine or attempt to censor the contents they distribute. Access Providers are not liable at all under civil or criminal law. They can only be ordered to block illegal contents by government agencies if it is commercially acceptable and if the agency is unable to enforce the law against the responsible Content or Service Provider.

In contrast, the CDA only restricts the civil liability of Access and Service Providers somewhat and rules out the criminal liability of Access Providers which would otherwise be imposed by sections 223(a) through (d) but not under other penal provisions.

\(^{162}\) Smedinghoff, \textit{supra} note 145, at 470.
4. **Administrative and Organizational Duties and Other Provisions for Online Providers**

The CDA does not lay down specific rules or duties which online service providers must fulfill. Instead, it simply defines criminal offenses, and the affected companies must decide how to organize their business or employee conduct to ensure that violations will not occur.

German legislators, however, traditionally impose their views on efficient compliance management by enacting extensive permit requirements and organizational duties.

a. **Permit Requirements**

A permit or license is only required for online services which qualify as television or radio broadcasting or regular phone service. European Community law bans national permit requirements for any other telecommunications service. After extensive debates over Internet telecommunications, the European Community Commission decided that "Internet phone service" does not qualify as "speech telephone service" under the respective directives and the German Telecommunications Act.

b. **Youth Protection Officers**

Service and Content Providers are required to designate a special youth protection officer for their organization unless there is no possibility that their services might cause danger to minors. This requirement would apply to any Service Provider who grants Internet access to a Content Provider dealing in erotic magazines or violent videos as well as to those Service Providers who do not closely regulate what their Content Providers are publishing.

c. **Information on the Identity of Content Providers**

German federal law requires a "professional" provider of Tele Services (commercial and non-profit organizations) to add its name and address to all contents published. According to state law, all

---

163. See § 4 TDG (see Part IIA.1 & note 1); § 4 MDStV, v. 20.5.1997 (Hessisches GVBl. I S.134, Berliner GVBl. I S.361); § 20 RStV, cited in RING, supra note 66, at C-0 StV.; SCHERER & BARTSCH, supra note 76, at 25.


providers of Media Services must add their names and addresses to all the material they publish. In addition, Content Providers of "electronic newspapers" (as defined in section 6 II MDStV) have to provide the name of an individual person (not a legal entity) residing in Germany who is responsible for everything the Content Providers publish.

d. **Anonymous Service for Users**

Access Providers must offer the possibility of anonymous activity to all Users and inform them of that option.  

66

e. **Data Protection**

In addition to the already strict general federal and state data protection laws,' there are specific rules for Tele and Media Services. Generally, personal data (data relating to private individuals) may not be collected and must be deleted immediately unless the data is absolutely necessary to provide services to the respective client or for payment processing. In that case, however, the User must be notified about which data is gathered and if such data is ever transferred to third parties. At any time, Users may request that their Access Provider provide an electronic statement listing all their personal data that has been gathered.

An Access Provider may not refuse to contract with customers on the basis that they deny use of their personal data for purposes other than merely providing the requested Tele or Media Services. User profiles for marketing purposes must be anonymous, so data may not be gathered, stored or forwarded with a link to the individual to whom it belongs. Tele and Media Services must be secure from infiltration or access by unauthorized third parties. Compliance with these provisions is supervised by special federal and state data protection agencies.

---

166. § 4 I Teledienstedatenschutzgesetz [Code on Data Protection in connection with Tele Services] [TDDSG], v. 22.7.1997 (BGBI. I S.1870-1879); § 13 I MDStV. This requirement is waived by an exception clause, if unacceptable in an individual case. Generally, with regard to commercial users, or at least with respect to services facilitating electronic commerce amongst commercial enterprises, an option of anonymous usership appears to be commercially unacceptable.

167. *See* Bundesdatenschutzgesetz [Federal Data Protection Code] [BDSG], v. 17.12.1997 (BGBI. I 3108). Section 36 BDSG requires the appointment of a data protection officer in any business that processes personal data through automated procedures and constantly employs five or more employees for that purpose.

168. §§ 12-17 MDStV; §§ 1-8 TDDSG.
f. Enforcement

Compliance with the above-mentioned requirements under the new federal and state Internet law can be enforced by the imposition of fines and the power to close businesses which fail to comply. Several federal, state and local authorities have jurisdiction over particular aspects of the field, including state media agencies, federal and state data protection agencies, state trade agencies, state police and others.

g. Extraterritorial Application

Although there is no precedent yet and the statutes do not specifically address this question, statutory organizational duties and permit requirements should be applied only to providers who base their activities in Germany, i.e., operate servers or offices in the German territory.

h. Right of Reply

Like most traditional German state laws on newspaper and broadcasting media and the European Community Broadcasting Directive on Television, section 10 MDStV grants a right to reply to anyone whose interests or reputation was damaged by statements of fact in electronic newspapers. The Content Provider must include a reply limited to factual corrections. The reply must be published in his Media Service free of charge. According to the BVerfG, provisions granting a right of reply against the press generally are not regarded as a violation of the freedom of speech protected by the German Constitution in article 51 GG.

Section 10 MDStV only applies to Content Providers based in

---


170. Landgericht Duesseldorf [Civil Law District Court], 1998 MMR, 370-77. But see Dirk M. Burton, Der Gegendarstellungsanspruch nach § 10 MDStV [The Right of Reply According to § 10 MDStV], 1998 MMR, 294, 296 (arguing that the right of reply should apply in connection with all content on the Internet and should not be limited to electronic newspapers).

Germany, but it grants the right of reply without regard to nationality and residence of the claimant. It is therefore available worldwide, for example, to any American citizen whose interests have been damaged by an electronic newspaper published on the Internet by a Content Provider whose operations are based in Germany. The right can be enforced in German civil courts by an application for an injunction. The claimant does not have to prove that the facts damaging his interests were incorrect, but there are certain other limitations to the claim such as deadlines and exceptions to avoid misuse.\textsuperscript{72}

\section*{III. Summary}

The new German Internet law contains substantial privileges for Access and Service Providers with regard to secondary liabilities arising from violations of general German criminal, civil, unfair competition and intellectual property law. Access Providers who simply set up Users with an online connection generally are not liable for the contents then made available to those Users. Service Providers are protected from liability as long as they do not knowingly use or allow their servers to be used to make illegal contents available to the public. These privileges apply worldwide to any international provider who might have otherwise violated German law. Providers based in Germany are required to comply with a number of administrative duties laid down by the new Internet law, such as strict data protection and the appointment of data and youth protection officers.

Unlike the CDA, the new German codes do not raise any new constitutional freedom of speech issues since the new German Internet law does not impose any new restrictions on the contents of speech and contains defenses available and acceptable not only to commercial providers but to everyone.

\textsuperscript{72} For example, § 10 MDStV requires that the claimant have a “justified interest” and the reply may not be inappropriately longer than the original statement. Additionally, publication cannot be enforced for replies stating facts that are obviously not true.