

1-1-1999

Case Update: German CompuServe Director Acquitted on Appeal

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, *Case Update: German CompuServe Director Acquitted on Appeal*, 23 HASTINGS INT'L & COMP. L. REV. 109 (1999).
Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol23/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.

Case Update: German CompuServe Director Acquitted on Appeal

BY LOTHAR DETERMANN*

This case note follows up on a previous article published in this law review about the managing director of the German CompuServe subsidiary, Mr. Felix Somm, who was indicted in 1996 and sentenced to two years imprisonment on probation in May 1998 by a judge in Munich.¹ In December 1999, the Munich court of appeals overruled the decision of the lower court and acquitted Mr. Somm.²

I. Crime and Punishment

The 1998 decision of the Munich court of first instance³ is

* Professor Dr. Lothar Determann practices international business law at Baker & McKenzie, San Francisco/Palo Alto; teaches Information Technology Law and E-Commerce Law at the University of San Francisco School of Law; and is a member of the Freie Universität Berlin law faculty as a private lecturer (Privatdozent).

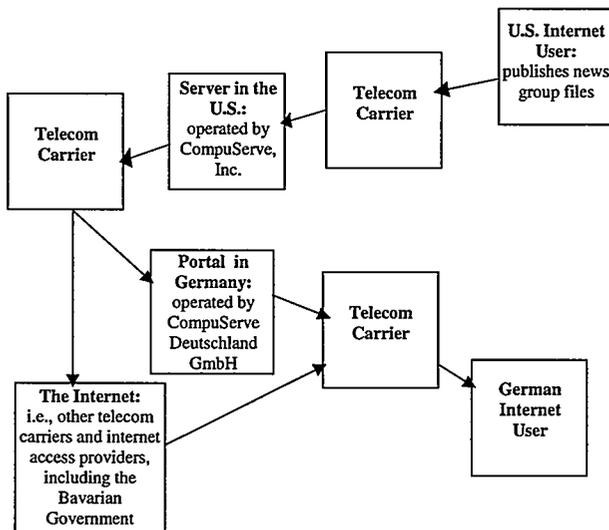
1. Lothar Determann, *The New German Internet Law*, 22 HASTINGS INT'L & COMP. L. REV. 113, 119 (1998).

2. LG München, NJW, 53 (2000), 1051 (with a case note by Hans-Heiner Kühne at 1003), CR, 20 (2000), 118 (with a case note by Hans-Werner Moritz at 119) (LG München Az. 20 Ns 465 Js 173158/95 (Dec. 28, 1999)) [hereinafter *Appeal Case*].

3. AG München, NJW, 51 (1998), 2836 (with a case note by Thomas Hoeren at 2792), CR 18 (1998), 500 (with a case note by Hans-Werner Moritz), MMR 1 (1998), 429 (with case note by Ulrich Sieber) (Az. 8340 Ds 465 Js 173158/95 (May 28, 1998)) [hereinafter *Lower Court Case*]. For additional information on the case, see 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], JURISTEN ZEITUNG 429 (1996) [hereinafter Sieber, *Criminal Liability*]; Ulrich Sieber, *Kontrollmöglichkeiten zur Verhinderung Rechtswidriger Inhalte in Computernetzen, Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups des Internet* [Possibility of Preventing Illegal Content in Computer Networks, For Example Newsgroups on the Internet, Implementation of §5 TDG], CR 17, (1997), 581 (653); Ulrich Sieber *Computerkriminalität und Informationsstrafrecht, Entwicklungen in der Internationalen Informations - und Risikogesellschaft* [Computer Criminality and

currently available in English on the Internet.⁴ Between 1995 and 1996, CompuServe Deutschland GmbH was a wholly owned subsidiary of CompuServe, Inc., a U.S. corporation. In 1995, CompuServe Deutschland GmbH had approximately 170 employees and was engaged in marketing, sales, customer service and technical support for its U.S. parent company in connection with the Internet services provided by CompuServe, Inc. CompuServe Deutschland GmbH participated in the distribution of content from U.S. servers to German Internet users by maintaining a dedicated telephone line between the servers of its parent company and Internet gateways in Germany. The German Internet users did not contract with CompuServe Deutschland GmbH, but rather directly with CompuServe, Inc., which offered, among other things, access to content on its servers. CompuServe, Inc. based and operated its servers in the United States. These servers contained content such as newsgroups with articles published by U.S. Internet users (content providers) and video games published by CompuServe, Inc.

Figure 1.



In December 1995, Munich law enforcement officials provided

Information Society, Developments in the International Information and Risk Society], CR (1995), 100.

4. See *German CompuServe Judgment Available On-Line*, (visited Sept. 5, 2000) <<http://www.qlinks.net/comdocs/somm.htm>> (unofficial translation); Cyber-Rights & Cyber-Liberties, *Felix Somm Decision in English*, (visited Sept. 5, 2000) <<http://www.cyber-rights.org/isps/somm-dec.htm>>.

CompuServe Deutschland GmbH with a list of 282 newsgroups emanating from CompuServe, Inc.'s servers, each of which contained child pornography and extreme violence. The Munich 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 official request. CompuServe, Inc. blocked the 282 newsgroups shortly thereafter to avoid sanctions against its subsidiary.

This block caused an uproar in the Internet community—especially in the United States—that impaired CompuServe's worldwide business.⁵ Therefore, in February 1996, 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 content. The District Attorney disagreed because distribution to adults of violent pornography and child pornography also violates German criminal laws (as well as some U.S. criminal laws). Although German law professors⁶ and politicians strongly criticized the proceedings of the Munich prosecutors, the prosecutors formally filed a bill of indictment against Mr. Somm in 1996.

On May 28, 1998, the Munich criminal court of first instance sentenced Mr. Somm, who had no previous police record, to two years' probation.⁷ This decision surprised many, including the Munich District Attorney, who had requested an acquittal of Mr. Somm after Germany enacted specific Internet laws in 1997. These laws applied retroactively and exempted Mr. Somm from criminal liability.⁸ Nevertheless, the Munich judge held that Mr. Somm was

5. See Berlin, *supra* note 3.

6. See, e.g., Sieber, *Criminal Liability*, *supra* note 3; Eric Hilgendorf, *Überlegungen Zur Strafrechtlichen Interpretation des Ubiquitaetsprinzips im Zeitalter des Internet* [*Considerations Regarding the Criminal Law Interpretation of the Principle of Ubiquity in the Age of the Internet*], 1997 N.J.W. 1873, 1874 (1997).

7. *Lower Court Case*, *supra* note 3; see also Mary Lisbeth D'Amico, *Germany Troubled by CompuServe Porn Conviction*, INDUSTRY STANDARD, May 29, 1998.

8. See LOTHAR DETERMANN, *KOMMUNIKATIONSFREIHEIT IM INTERNET* [FREEDOM OF COMMUNICATIONS ON THE INTERNET] 575-92 (1999) (English summary

guilty of thirteen counts of violating section 184 III of the German Penal Code (StGB)⁹ 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)¹⁰ 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)¹¹ 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 telephone line and gateways operated by CompuServe Deutschland GmbH. Through the same connection, German customers of CompuServe, Inc. also continued to have access to extremely violent video games that had been rated PG-18 by the competent German agency.¹²

There is little doubt that the contents in question did indeed qualify as illegal materials under German and United States criminal law and that the defendant helped distribute them. Without the specific limitations provided by the 1997 German Internet laws, a conviction might arguably have been justified, although German criminal law scholars came to the contrary conclusion in articles published during the 1996 proceedings and shortly after the 1998 judgment.¹³ Under the specific German Internet laws, however, Mr. Somm was clearly exempt from criminal liability, which even the District Attorney conceded in his 1997 request for an acquittal.

II. The Acquittal

The Munich court of appeals also found that Mr. Somm was exempt from liability under the 1997 German Internet laws and also

on 617, 623). An English translation is available at <<http://www.usfca.edu/ipla/determann-article.htm>>]; see generally NORBERT WIMMER & GERHARD MICHEAL, DER ONLINE-PROVIDER IM NEUEN MULTIMEDIARECHT [THE ONLINE PROVIDER UNDER NEW MULTI MEDIA LAW] (1998).

9. § 184 III StGB, v. 26.1.1998 (BGBl. I S.1607).

10. Gesetz ueber die Verbreitung jugendgefährdender Schriften [GjS] [Law Against the Distribution of Materials Endangering Minors], v. 28.10.1998 (BGBl. I S.3186).

11. *Lower Court Case*, *supra* note 3, at 22-27.

12. The Bundesprüfstelle zum Schutz vor Jugendgefährdenden Schriften [Federal Censorship Commission for Materials Endangering Minors] publishes a list of materials that may not be made accessible to minors. See § 1 GjS.

13. See, e.g., Sieber, *Criminal Liability*, *supra* note 3.

that Mr. Somm's contributions to the publication of the illegal content were not even actionable under traditional German criminal laws.¹⁴

1. Traditional German Criminal Laws

Mr. Somm did not qualify as an accomplice, principal in the second degree, or accessory to the crimes because he lacked specific control over the publications. Customers of CompuServe, Inc. posted the illegal materials on CompuServe, Inc.'s servers. These private individuals acted as principals in the first degree. CompuServe, Inc. was technically able to block or remove these postings once it discovered their nature. Therefore, one could argue that CompuServe, Inc. aided these principals and thus qualified as an accomplice or principal in the second degree. However, CompuServe Deutschland GmbH, managed by Mr. Somm, was physically unable to block or remove specific postings from its parent company's servers. As managing director, Mr. Somm basically had only one possibility to influence the dissemination of the illegal content through the Internet connection maintained by CompuServe Deutschland GmbH: he could have ordered the employees of CompuServe Deutschland GmbH to block the entire link between the German Internet users and CompuServe, Inc.'s servers. Obviously, this would likely have resulted in his immediate removal as managing director of CompuServe Deutschland GmbH by its sole shareholder, CompuServe, Inc. Even if Mr. Somm had taken this drastic action, the illegal postings on CompuServe, Inc.'s servers would still have remained accessible to German Internet users via connections provided by other Internet hosting service providers, including CompuServe's competitors and, most notably, the Bavarian government. In light of these factual and legal circumstances, the Munich court of appeals held that Mr. Somm's actions or omissions did not legally qualify as a significant aid to the distribution of the illegal content. Consequently, Mr. Somm did not commit an *actus reus*, the first basic element of any crime.

In addition, the Munich court of appeals held that Mr. Somm lacked the *mens rea* required by the applicable German criminal statutes.¹⁵ All but one charge required that Mr. Somm have acted, or have failed to act, with at least general intent. In this regard, the

14. *Appeal Case*, *supra* note 2, at 29-30.

15. *Id.* at 30, 32.

court of appeals stressed that Mr. Somm continuously urged CompuServe, Inc. to block or remove the illegal postings from its servers. However, in this, the court of appeals went too far. Under general principles of criminal law a personal *preference* to avoid the illegal results of an action or omission does not negate general intent. General intent only requires that the defendant act with the knowledge that his actions or omissions will cause the illegal results that constitute an element of the crime, regardless of whether the defendant welcomes or fears such results. When informed by the prosecutors that the illegal postings existed, Mr. Somm had such knowledge. Therefore, he acted intentionally when he failed to block the connection to CompuServe, Inc.'s servers. Mr. Somm did not lack *mens rea*.

This is even clearer with regard to the charge of negligent failure to prevent access of minors to violent computer games. When the Munich court of appeals stressed that Mr. Somm could not be required to permanently check the nature of more than one thousand computer games available on CompuServe, Inc.'s servers,¹⁶ the court overlooked the fact that Mr. Somm was only indicted for not preventing access to certain games that were specifically listed and described by the Munich district attorneys in their written notice to CompuServe Deutschland GmbH. Furthermore, Mr. Somm intentionally refrained from blocking access to CompuServe, Inc.'s servers altogether.

Therefore, while the Munich court of appeals correctly negated an *actus reus*, it had no grounds to negate the respective *mens rea*.

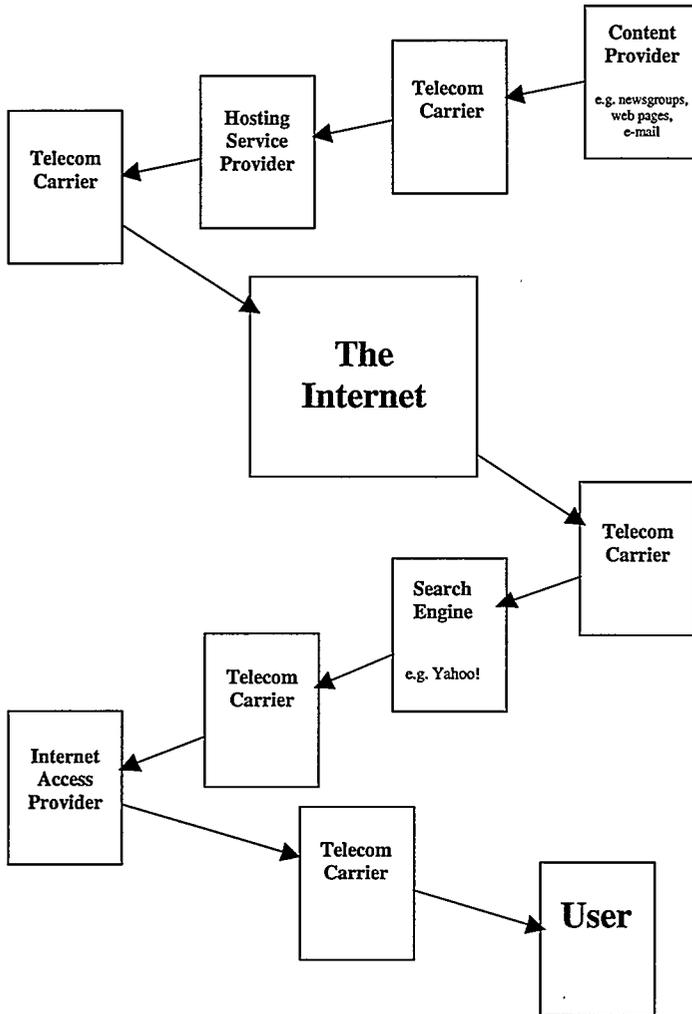
2. *The 1997 German Internet Laws*

Even assuming that an *actus reus* occurred *and* *mens rea* existed, Mr. Somm was exempt from criminal liability under the 1997 German Internet laws.¹⁷ These laws divide the roles of the players on the Internet into five categories: content providers, access providers and hosting service providers (collectively referred to as online providers), telecommunications carriers and users.

16. *Id.*

17. *Id.* at 31.

Figure 2.



a. Content, Access and Hosting Service Providers

Content providers and users are the cyberspace equivalents of traditional speakers and the audience.¹⁸ The content provider selects and publishes information that is made available to the user. The content provider uses the computer (server), online connections and software of a hosting service provider to publish this information on

18. See *ACLU v. Reno*, 929 F. Supp. 824, 843 (E.D. Pa. 1996), *aff'd*, *Reno v. ACLU*, 117 Sup. Ct. 2329 (1997); see also Telecommunications Act of 1996 § 509, 47 U.S.C. § 230(f)(3) (1996) (defining "Information Content Provider").

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 content disseminated through, 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., telephone companies and television cable operators.

In this role, telecommunications carriers fulfill similar functions to their traditional telephone business, and it is not apparent why the rules regarding their liabilities and responsibilities as applied to Internet communications should be treated differently. 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.¹⁹ There is also no apparent reason why content providers and users should be treated differently from off-line speakers and audiences. Before the 1997 German Internet laws were enacted it was questionable, however, to what extent, if any, classic media roles, such as editors, news agents or telephone companies,²⁰ are comparable to access and hosting service providers. For purposes of clarification, the 1997 German Internet laws provide specific rules in this area that are somewhat similar to the rules set forth in the U.S. Communications Decency Act,²¹ and the Digital Millennium Copyright Act.²²

In Mr. Somm's case, U.S. customers of CompuServe, Inc. posted materials on CompuServe, Inc.'s servers. In this role, CompuServe, Inc. acted as a hosting service provider for its customers, the content providers. CompuServe Deutschland GmbH was not involved at all

19. See Ruth Hill Bro, *Defamation Online*, in *ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET* 429, 441 (Thomas J. Smedinghoff ed., 1996).

20. See generally R. Hayes Johnson, Jr., Note, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in Stratton Oakmont, Inc. v. Prodigy Services Co.*, 49 ARK. L. REV. 589 (1996); *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991); *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 805178, at *10 (N.Y. Sup. Ct. Dec. 11, 1995), 24 MEDIA L. REP. 1126 (N.Y. Sup. Ct. 1995); AG Berlin, CR 18 (1998), 111 (260-DS 857/96 (June 30, 1997)).

21. Telecommunications Act of 1996, 47 U.S.C. §§ 223-230 (1996); see generally *Reno v. ACLU*, 117 S. Ct. 2329, 2347-48 n.45 (1997); *Shea v. Reno*, 930 F. Supp. 916, 941 (S.D.N.Y. 1996); Carl Benson et al., *Computer Crimes*, 34 AM. CRIM. L. REV. 409, 421 (1998).

22. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

in this relationship and therefore did not qualify as a hosting service provider. 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 Internet access provider. CompuServe Deutschland GmbH supported CompuServe, Inc. as an access provider by providing technical support and maintaining a dedicated telephone line. Therefore, CompuServe Deutschland GmbH qualified only as an Internet access provider.²³

b. Liability of Internet Hosting Service Providers

Under the 1997 German Internet laws, a hosting service provider such as CompuServe, Inc. is only liable for illegal content that it channels onto the Internet if (1) it is actually aware of the substance of the illegal content, and (2) if it is technically possible and reasonably acceptable for the hosting service provider to prevent the publication or distribution of the unlawful content on the Internet.

The statute does not define the term “acceptable.” This term appears in many other German statutes, however, and it is generally interpreted to necessitate a balancing of conflicting interests.²⁴ When proposing the 1997 draft legislation,²⁵ the German federal government explicitly suggested such an interpretation of the term “acceptable.”²⁶ According to the German federal 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 hosting service provider, the government specifically referred to the case of a hosting service provider that made several newsgroups available and was asked to block an entire newsgroup because of illegal content in a few individual files posted there.²⁷ Thus, arguably German federal law did not mandate that CompuServe, Inc. block the illegal content in this case. 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 reasonably acceptable to

23. See *Appeal Case*, *supra* note 2, at 31 (overruling the opinion of the lower court on this point).

24. See BT-Drs 13/7385, 20.

25. *Id.* (containing information on the legislative process according to the federal constitution).

26. *Id.*

27. *Id.*

CompuServe, Inc. However, given the extremely negative effects of child pornography and the relatively minor expenses for blocking, one might also come to the contrary conclusion with regard to this case and CompuServe, Inc.

c. Liability of Internet Access Providers

Under the 1997 German Internet laws, an Internet access provider (such as CompuServe Deutschland GmbH in this scenario)²⁸ is generally *not* liable for the contents to which it provides access. However, an Internet 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 provider or hosting service provider (because, e.g., they live abroad).

It is questionable whether, under these rules, an Internet access provider could be exempt from liability even if it has knowledge of the illegal content it has made available. The legislature answered this question in the affirmative. Otherwise, the differentiation between Internet access providers and hosting service providers would have been unnecessary.²⁹ Accordingly, CompuServe Deutschland GmbH and its director, Mr. Somm, were exempt from criminal liability, even though they had knowledge of the illegal postings.³⁰ This was the conclusion of the Munich court of appeals, which based its acquittal of Mr. Somm also on the 1997 German Internet laws.³¹

III. Outlook—New EC Laws on Online Provider Liability

In the first three years since the 1997 privileges for online providers have been in effect in Germany, police and district attorneys seemed to have backed off from prosecuting Internet access providers and Internet hosting service providers. German civil law courts have either applied the new rules very reluctantly or

28. See *Appeal Case*, *supra* note 2, at 31.

29. See Thomas Hoeren, *Anmerkung* [*Case Note*], 1998 M.M.R. 97-98 (1998).

30. See the German Federal Attorney General's formal reasons for terminating criminal proceedings against an access provider in the decision, November 26, 1997, 2 BJS104/96-4, 1998 MMR 93-98 (1998). This view is heavily criticized by Thomas Hoeren. See Hoeren, *supra* note 30.

31. *Appeal Case*, *supra* note 2, at 31.

overlooked them altogether.³² The Munich court of appeals in Mr. Somm's case also expressed little respect for the new rules and the underlying legislative intent.³³ Nevertheless, the German statutory privileges for Internet access providers and hosting service providers are likely to remain applicable in the foreseeable future because they are in compliance with the European law, which is about to come into effect.

The European Community (EC)³⁴ has recently adopted a final version of a Directive on "certain legal aspects of information society services, in particular electronic commerce, in the internal market,"³⁵ commonly referred to as the "E-Commerce Directive."³⁶ Once the EC has formally enacted the E-Commerce Directive, the EC Member States, including Germany, must conform their national laws to the rules of the directive within eighteen months, i.e., probably before the end of the year 2001.

Section 4 of the E-Commerce Directive is entitled "Liability of Intermediary Service Providers" and contains rules that would apply in situations like the case against Mr. Somm:

Article 12 "Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information

32. See, e.g., OLG München, CR 18 (1998), 300; OLGZ München, K&R 2 (1999), 335; LG Hamburg, ZUM—RD 18 (1998), 389; LG Potsdam, K&R 2 (1999), 428 (429); LG Frankfurt, CR 19 (1999), 45 (46) (with case note by Kloos, CR 1999 at 46). See Lothar Determann, *Abgrenzung gesetzlicher Medienkategorien im Internet – IuKDG-Bericht der Bundesregierung und Probleme der Praxis [Differentiation Between Legal Media Categories on the Internet—IuKDG Report of the Federal Government and Practical Problems]*, Rtkom, 52 (2000), 11.

33. *Appeal Case, supra* note 2, at 30-31.

34. While the European Union (EU) provides a common "roof" for the different forms of cooperation of its Member States, it is still the EC that passes the relevant laws and undertakes nearly all other relevant legal actions.

35. 2000 O.J. (C128) 32.

36. See generally LOTHAR DETERMANN & CHRISTOPH RITTWEGER, EC ELECTRONIC BUSINESS LAWS (forthcoming) (manuscript on file with the authors); Gerald Spindler, *Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-Commerce Richtlinie [Liability of Service Providers Under the Proposed E-Commerce Directive]*, 1999 M.M.R. 199 (1999); Hubertus Gersdorf, *E-Commerce und Rundfunk [E-Commerce and Broadcasting]*, 1999 RTkom 75 (1999); Thomas Hoeren, *Vorschlag für eine EU-Richtlinie über E-Commerce [The Proposed E-Commerce Directive]*, 1999 M.M.R. 192 (1999); Hans-Georg Landfermann, *Der Richtlinienentwurf Elektronischer Geschäftsverkehr- Ziele und Probleme [The Proposed E-Commerce Directive—Goals and Problems]*, 1999 Z.U.M. 795 (1999).

provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13. 'Caching'

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

- (a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 'Hosting'

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public

authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Under the E-Commerce Directive, CompuServe, Inc. would qualify as a hosting service provider (Article 14) and CompuServe Deutschland GmbH as a provider of “mere conduit” and “caching” (Articles 12 and 13).

According to Article 15 of the E-Commerce Directive, neither CompuServe, Inc., CompuServe Deutschland GmbH, nor Mr. Somm may be obligated to monitor the content posted by their customers on CompuServe, Inc.’s servers. Also, they would generally not be liable for any illegal content posted by their customers until they have actual knowledge of such illegal postings.

However, Articles 12(3), 13(2), and 14(3) of the E-Commerce Directive would not preclude German government authorities from requesting either CompuServe, Inc. or CompuServe Deutschland GmbH from preventing further dissemination of illegal contents by blocking access or removing postings. Consequently, under the E-Commerce Directive, EC Member States could enact national laws allowing their national attorneys general to demand that a provider of a “mere conduit” (such as CompuServe Deutschland GmbH in the case against Mr. Somm) prevent access to servers displaying illegal content altogether (such as CompuServe, Inc.’s servers in the case against Mr. Somm). If a provider of a “mere conduit” fails to comply with a EC Member State’s law enforcement official’s request, the E-Commerce Directive would not warrant any privileges with respect to vicarious liabilities arising under national laws. As a result, as far as EC law is concerned, under such circumstances—e.g., under the facts of the case against Mr. Somm—the Internet access provider and its managers could be punished under national laws if national laws so provide.

IV. Conclusion

The 1997 German Internet laws as applied by the Munich court of appeals in Mr. Somm’s case seem to adequately protect Internet hosting service providers and Internet access providers from liabilities for postings of illegal materials by their customers. Under current German law, companies that only provide access to the Internet, or a

“mere conduit,” are generally not liable for any illegal content on third parties’ servers to which they provide access.

The 2000 E-Commerce Directive of the European Community does not afford any additional protection in such scenarios. It allows the EC Member States to enact laws that provide a standard of protection similar to that of the 1997 German laws, but it also allows national laws that are less protective of online providers.
