

# ALAI 2001 Congress, New York: Adjuncts and Alternatives to Copyright

## Session I.D.2: The Scope of the Prohibition on Circumvention of Technological Measures – Exceptions

GERMANY

National Reporter: Peter Wand\*

### I. State of the law before transposition of the WIPO Treaties

1.1. Before adoption of the WIPO Treaties in 1996, did your country already have legislation concerning technological protection of copyrighted works? If so, in what areas (e.g. software, etc.)?

Art. 7(1) lit. c of the EU Directive on the Legal Protection of Computer Programs (the “Computer Program Directive”)<sup>1</sup> obliges Member States to provide for appropriate measures against

*“[...] any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.”*

Germany implemented the Computer Program Directive in 1993.<sup>2</sup> Art. 7(1) lit. c of the Computer Program Directive became § 69f(2) of the German Copyright Act (*Urheberrechtsgesetz*, the “UrhG”).

1.2. Did your country already have legislation addressing protection of information encoded in the work, concerning the work or its author or copyright owner?

Germany does not have legislation specifically addressing the protection of information encoded in the work, which pertains to the work or its author or copyright owner. However, such information may form an integral part of a technical device applied to protect a computer program.<sup>3</sup> In so far, it is covered by § 69f(2) UrhG.

1.3. Did your country’s legislation prohibit the circumvention of technological measures:

1. By the person who committed the act of circumvention?

Sec. 69c, first sentence, no. 2 UrhG, another provision in the German Copyright Act based on the Computer Directive, gives the right holder the exclusive right to adapt a computer program and reproduce the results thereof. Whereas, according to § 23 UrhG, the adaptation or transformation of other kinds of works is permitted in principle, and the right holder’s consent is required only for their publication or exploitation, in the case of computer programs, adaptations or transformations may only be made by or with the authorization of the right holder. Although this provision does not expressly prohibit the circumvention of technological measures, courts have found that any circumvention of technical devices requiring the alteration of a computer program would violate the provision.<sup>4</sup> As the right of

---

\* Dr. jur., LL.M. (Columbia), Attorney-at-Law, Cleary, Gottlieb, Steen & Hamilton, Frankfurt am Main. The author would like to thank his colleague Lenora Bonéy, J.D. (Columbia), for her valuable comments.

<sup>1</sup> Council Directive 91/250 of May 14, 1991 on the Legal Protection of Computer Programs (the “Computer Program Directive”), OJ 1991 L 122/42.

<sup>2</sup> Zweites Gesetz zur Änderung des Urheberrechtsgesetzes vom 9.6.1993 [Second Law for the Amendment of the German Copyright Act of June 9, 1993], Bundesgesetzblatt (“BGBl”), Teil I, p. 910.

<sup>3</sup> See Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELY TECH. L.J. 161 *et seq.* (1997).

<sup>4</sup> OLG Karlsruhe, NEUE JURISTISCHE WOCHENSCHRIFT (“NJW”) 49 (1996), 2583 (2584); LG Düsseldorf, COMPUTER UND RECHT (“CR”) 12 (1996), 737 (739), *aff’d*, OLG Düsseldorf, CR

adaptation in § 69c, first sentence, no. 2 UrhG is an exclusive right under copyright law, damages and injunctive relief can be sought under § 97(1) UrhG.

2. *By the person who furnished the means of circumvention:*
  - a. *By furnishing information about these means?*
  - b. *By furnishing the devices enabling the circumvention (preparatory acts)?*
  - c. *By offering circumvention services?*

Sec. 69f(2) UrhG is directed at the furnishing of means enabling circumvention and entitles the right holder to demand destruction of such means. It provides for § 69f(1) UrhG to apply *mutatis mutandis*. If one incorporated the first sentence of § 69f(1) UrhG into § 69f(2) UrhG, the latter would read as follows:

*The right holder may require from the owners or proprietors that any means, the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device applied to protect a computer program, be destroyed.*

The mere provision of information about such means is not prohibited by § 69f(2) UrhG. However, detailed descriptions of how to circumvent a technical device, for example, so-called unprotect guidelines,<sup>5</sup> may be considered means of circumvention.

As an example of a means of circumvention, the legislative materials refer to copying programs capable of deactivating the copy protection applied to a computer program protected under copyright law.<sup>6</sup> So far, court decisions addressing § 69f(2) UrhG have dealt with programs that were used to circumvent so-called dongles.<sup>7</sup> A dongle is an anti-copying device that attaches to a computer, typically on a parallel port, and must be present in order to run a particular computer program.<sup>8</sup> Circumvention services appear not to be covered by § 69f(2) UrhG as they cannot be owned or possessed.

Sec. 69f(2) UrhG in connection with the second sentence of § 69f(1) UrhG provides for § 98(2) and (3) UrhG to apply *mutatis mutandis*. Thus, right holders may require that any means of circumvention be surrendered to them in return for equitable remuneration, which may not exceed the cost of manufacture. Where this would lead to disproportionate results for the owner or the proprietor, and if the ability to circumvent can be eliminated in some other way, right holders may only demand the measures necessary for such elimination.

1.4. *In the absence of legislation, have judicial decisions prohibited acts such as:*

1. *The act of circumvention?*
2. *Furnishing devices to enable circumvention?*
3. *Furnishing circumvention services?*

There appears to be no case law in Germany prohibiting the act of circumvention, except if a computer program is altered in order to circumvent technical devices (see 1.3.1. above).

---

13 (1997), 337 (339). See also Wilhelm Nordemann & Kai Vinck, in WILHELM NORDEMANN ET AL., URHEBERRECHT, § 69c UrhG no. 4 (9<sup>th</sup> ed. 1998).

<sup>5</sup> PETER WAND, TECHNISCHE SCHUTZMASSNAHMEN UND URHEBERRECHT, EIN VERGLEICH DES INTERNATIONALEN, EUROPÄISCHEN, DEUTSCHEN UND US-AMERIKANISCHEN RECHTS [Technical Protection Measures and Copyright, A Comparison of International, European, German and U.S. Law] 71 (2001).

<sup>6</sup> Entwurf eines Zweiten Gesetzes zur Änderung des Urheberrechtsgesetzes der Bundesregierung v. 18.12.1992 mit amtlicher Begründung [Draft of Second Law to Amend the Copyright Act by the Federal Government dated December 18, 1992, including the official reasoning], Bundestagsdrucksache 12/4022, p. 15.

<sup>7</sup> OLG Karlsruhe, CR 12 (1996), 341 (343); LG Düsseldorf, CR 12 (1996), 737 (738) “Dongle-Umgehung“ [Dongle Circumvention], *aff’d*, OLG Düsseldorf, CR 13 (1997), 337 (339).

<sup>8</sup> DOUGLAS A. DOWNING, ET AL., DICTIONARY OF COMPUTER AND INTERNET TERMS 138 (6<sup>th</sup> ed. 1998).

Theoretically, a person who circumvents a technical device applied to protect a work or furnishes the means or services necessary for doing so may be held liable for copyright infringement under the German Copyright Act. Although the circumvention of such technical devices as well as the sale of copying equipment used for infringement is probably better referred to as contributory copyright infringement (*mittelbare Urheberrechtsverletzung*), such a term is virtually non-existent in German copyright law. Whereas the doctrine of contributory infringement is explicitly referred to in § 10 of the German Patent Act (*Patentgesetz*, the “PatG”),<sup>9</sup> the German Copyright Act does not provide a similar reference. Unlike the U.S. Supreme Court,<sup>10</sup> the German Federal Supreme Court (*Bundesgerichtshof*, the “BGH”) did not borrow precedent from German patent law in making its decisions regarding tape-recorders, blank tapes and copy shops, but simply referred to a general principle of civil law according to which anyone who unlawfully interferes with a right that is enforceable against the general public may be held liable for such interference.<sup>11</sup>

The circumvention of a technical measures applied to protect a work is, in principle, only a preparatory act. It facilitates infringement, but generally does not constitute an infringement in itself. Apart from the primary infringer, anyone who circumvents such technical measures or provides the means or services necessary for doing so, thereby bringing about an infringement, should also be liable for what is called contributory infringement in this report if there is an adequate causal connection between the objectionable conduct and the infringement. However, there is an important limitation to this rule. In cases relating to tape-recorders, blank tapes and copy shops, German courts have found contributory infringement to be present in such circumstances, but have decided that the right holders may only demand reasonable measures to prevent infringement, since these means could be used to a considerable degree for legitimate purposes. Thus, the persons furnishing the equipment were ordered only to indicate clearly to the persons using the equipment that the exclusive rights under copyright and neighboring rights law had to be observed.<sup>12</sup> From this limitation it becomes clear that the doctrine of contributory infringement does not appear to provide adequate legal protection against circumvention of technical measures.

By contrast, § 1 of the German Unfair Competition Prevention Act (*Gesetz gegen den unlauteren Wettbewerb*, the “UWG”)<sup>13</sup> is of particular significance for the legal protection of technical measures against circumvention. German courts have applied this provision to enjoin third parties from the unauthorized offer or distribution of means for the circumvention of measures designed to prevent the infringement of copyright and neighboring rights law<sup>14</sup> as well as for the circumvention of access control measures.<sup>15</sup> The courts thereby reverted to different concepts all directed against free-riding. Possible remedies under § 1 UWG include injunctive relief and damages. Under certain circumstances, the court may also order the destruction of the means of circumvention.

It should be noted, however, that § 1 UWG requires a competitive relationship (*Wettbewerbsverhältnis*)

---

<sup>9</sup> BGBl. 1981, Teil I, p. 1, as last amended by law of December 22, 1999, BGBl. 1999, Teil I, p. 2598.

<sup>10</sup> Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

<sup>11</sup> BGH, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT (“GRUR”) 57 (1955), 492 (500) “Grundig-Reporter”; BGH, GRUR 62 (1960), 340 (343) “Werbung für Tonbandgeräte” [Advertising for Tape Recorders]; BGH, GRUR 66 (1964), 91 (92) “Tonbänder-Werbung” [Advertising for Tapes]; BGH, GRUR 66 (1964), 94 (96) “Tonbandgeräte-Händler” [Tape Recorder Dealers]; BGH, GRUR 67 (1965), 104 (105) (“Personalausweise” [Identity Cards]; BGH, GRUR 67 (1965), 686 (687) “Magnettonband II” [Magnetic Tape II]; BGH GRUR 86 (1984), 54 (55) “Kopierläden” [Copy Shops].

<sup>12</sup> BGH, GRUR 62 (1960), 340 (344); BGH, GRUR 66 (1964), 91 (92); BGH, GRUR 66 (1964), 94 (96); BGH, GRUR 67 (1965), 686 (688); BGH, GRUR 67 (1965), 104 (107); BGH, GRUR 86 (1984), 54 (55-56).

<sup>13</sup> RGBl. p. 499, as last amended by law of June 27, 2000, BGBl. 2000, Teil I, p. 897.

<sup>14</sup> OLG Stuttgart, CR 5 (1989), 685-688 “Feilhalten von Hardlock-Entfernern” [Offering of Hardlock Removing Devices]; OLG Düsseldorf, GRUR 91 (1989), 535-536 “Hardware-Zusatz” [Auxiliary Hardware]; LG München, CR 11 (1995), 669-671 “Dongle”, *aff’d*, OLG München, CR 12 (1996), 11-18 “Dongle”, *aff’d*, BGH GRUR 98 (1996), 78-79; OLG München, CR 11 (1995), 663-665 “UNPROTECT”.

<sup>15</sup> OLG München, CR 9 (1993), 31 “Multifilter”; OLG Frankfurt am Main, NJW 49 (1996), 264-265 “Piratenkarte” [Pirate Card].

between the parties.<sup>16</sup> This may lead to a lack of protection with respect to the distribution of means of circumvention by private individuals.<sup>17</sup> Moreover, it should be noted that generally only an injured competitor has the standing to sue.<sup>18</sup> Non-injured competitors, economic and consumer associations are limited to actions for injunctive relief under § 13(2) UWG.

1.5. *If your country had, by legislation or judicial decision, prohibited circumvention of technological measures, did this prohibition prove effective?*

Sec. 1 UWG is the provision most commonly used with respect to means of circumvention in Germany. Although § 69f(2) UrhG was discussed in a few German court decisions,<sup>19</sup> it appears that it has never been used as a basis for a court order relating to circumvention devices. Sec. 69c, first sentence, no. 2 UrhG was employed in two actions ordering the defendants to cease offering their services for the removal of the copy protection code from the plaintiff's computer programs.<sup>20</sup> The doctrine of contributory infringement has never been applied by German courts to means of circumvention.

1.6. *In the absence of legislation or judicial decisions, did a practice of tolerating circumvention develop?*

As German law is not directed against circumvention, with the exception of § 69c, first sentence, no. 2 UrhG, circumvention has been tolerated.

1.7. *Did your country's legislation provide for exceptions to prohibitions on circumvention? If so, please describe them.*

German law does not provide for any explicit exceptions to § 69(2) UrhG. Secs. 69d and 69e UrhG merely contain exceptions to the acts referred to in § 69c UrhG. When the Computer Program Directive was implemented, the legislature was aware of the fact that the relationship between this provision and the exceptions to the exclusive rights under copyright law remained unclear, but left it to the courts and academia to solve the problem.<sup>21</sup>

One might be tempted to read the exceptions to the exclusive rights under copyright law into § 69f(2) UrhG. In support of this, it could be argued that § 69a *et seq.* UrhG relate to the copyright protection of computer programs. Sec. 69f(2) UrhG aims to enforce this protection and should therefore reach no further than copyright itself. Moreover, something that cannot be prevented by means of a contract should not be made *de facto* impossible. Thus, at least the exceptions relating to computer programs, which may not be waived by contract according to § 69g(2) UrhG, should also be mandatory exceptions to the prohibition under § 69f(2) UrhG.

Based on this reasoning, it has been assumed in relation to § 69d(1) and (2) UrhG that § 69f(2) UrhG does not apply to means of circumvention which can be used for correcting errors or making back-up copies.<sup>22</sup>

However, this view should be rejected.<sup>23</sup> It does not provide for effective legal protection and allows

---

<sup>16</sup> See WOLFGANG HEFERMEHL & ADOLF BAUMBACH, WETTBEWERBSRECHT, Einl UWG no. 247 (2001).

<sup>17</sup> MICHAEL LEHMANN, *Electronic Commerce und Urheberrecht*, in RECHTSGESCHÄFTE IM NETZ – ELECTRONIC COMMERCE 105, 110 (1999).

<sup>18</sup> WOLFGANG HEFERMEHL & ADOLF BAUMBACH, *supra* note 16, Einl UWG no. 293.

<sup>19</sup> LG München, CR 11 (1995), 669-671, *aff'd*, OLG München CR 12 (1996), 11-18; OLG Karlsruhe CR 12 (1996), 341 (342); LG Düsseldorf, CR 12 (1996), 737 (739), *aff'd*, OLG Düsseldorf, CR 13 (1997), 337 (339).

<sup>20</sup> *See supra* note 4.

<sup>21</sup> Draft of Second Law to Amend the Copyright Act by the Federal Government, *supra* note 6, p. 12.

<sup>22</sup> Andreas Raubenheimer, *Vernichtungsanspruch gem. § 69f UrhG*, CR 10 (1994), 129 (131), and *Beseitigung/Umgehung eines technischen Programmschutzes nach UrhG und UWG*, CR 12 (1996), 69 (72).

<sup>23</sup> Ulrich Loewenheim, in GERHARD SCHRICKER (ed.), URHEBERRECHT, § 69f UrhG no. 11 (2d. ed. 1999).

for excuses, which are very difficult to refute. Users would be granted a self-help right to circumvent technical devices applied to protect computer programs.

It appears more sensible to look at the reasoning behind an exception to the exclusive rights under copyright in order to determine whether this exception should be applied to § 69f(2) UrhG. The fact that § 69g(2) UrhG provides that some exceptions can not be waived by contract, should merely be understood to be an indication of a corresponding exception to § 69f(2) UrhG. In the interest of providing effective legal protection for technical devices applied to protect computer programs, the user should be asked to bring a claim instead of relying on an exception whenever the exception corresponds with a right of the user.<sup>24</sup> Such a claim may result from a contract, statutory warranty regulations or the exception itself.

For example, in the opinion of the BGH, a program interlock might be considered to be a fault in the software.<sup>25</sup> In the court's view, this would depend on the specific circumstances, especially on whether the program requires protection and whether the user is able to use it without restriction as contractually specified. The Higher Regional Court of Düsseldorf considered the installation of a program interlock to be a serious contract infringement, justifying the immediate termination of the software license agreement if, for professional purposes, the user requires unrestricted access at all times to the data processed by the program.<sup>26</sup> The Higher Regional Court of Celle decided that dongle-related system crashes are faults within a computer program.<sup>27</sup> One commentator infers from § 69d(2) UrhG that the purchaser of a program has a contractual right to be provided with a backup copy of the program.<sup>28</sup>

An exception to this is found in § 69e UrhG. Giving priority here to the protection against circumvention would jeopardize the intended freedom of access to the markets.<sup>29</sup> The Regional Court of Düsseldorf fails to recognize this when, by citing § 69e(1) UrhG, it considers the circumvention of a technical device to protect computer programs to violate § 69e(3) UrhG.<sup>30</sup> According to § 69e(3) UrhG, subsections (1) and (2) must be interpreted in such a way that their application neither impairs the normal exploitation of the work nor unreasonably prejudices the right holder's legitimate interests.

The loss of a dongle as a result of fire or theft is no legal justification for the circumvention of technical devices to protect computer programs.<sup>31</sup> In the absence of any contractual provisions to the contrary, the risk of loss lies solely with the program user.

## **II. Implementation of WIPO Treaty obligations – provisions concerning the protection of technological measures.**

*2.1. Has your country adopted legislation to implement the obligations set forth in the WIPO Treaties (Arts. 11 and 12 of the WIPO Copyright Treaty; Arts. 18 and 19 of the WIPO Performers and Phonograms Treaty)?*

1. *When?*
2. *By what means? A special copyright law? A general law of which copyright legislation is only a part?*

Awaiting the adoption of the EU Directive on Copyright and Related Rights in the Information Society ("the Copyright Directive"), Germany has not yet transposed the WIPO Treaties into national law. As a first step towards implementing legislation, the German Federal Ministry of Justice published a discussion draft of a law for the amendment to the German Copyright Act in July 1998. The discussion

---

<sup>24</sup> PETER WAND, *supra* note 5, p. 148.

<sup>25</sup> BGH, NJW 50 (1987), 2004 (2005) "Programmsperre II" [Program Interlock II].

<sup>26</sup> OLG Düsseldorf, BETRIEBSBERATER ("BB") 48 (1993), Supp. 13, 6 (7).

<sup>27</sup> OLG Celle, CR 10 (1994), 217 (218).

<sup>28</sup> Ulrich Loewenheim, *supra* note 23.

<sup>29</sup> PETER WAND, *supra* note 5, p. 149.

<sup>30</sup> LG Düsseldorf, CR 12 (1996), 737 (739).

<sup>31</sup> LG Frankfurt am Main, CR (1997), 25; LG Düsseldorf, CR 12 (1996), 737 (739), *aff'd*, OLG Düsseldorf, CR 13 (1997), 337 (339).

draft included provisions regarding the protection of technological measures and rights management information.<sup>32</sup> The draft was based on the EU Commission's initial proposal for the Copyright Directive of December 10, 1997.<sup>33</sup> The German discussion draft was to be continuously updated in order to reflect the amendments in the proposal for the Copyright Directive. Although the German Federal Minister of Justice announced the intended release of a revised draft in March 1999<sup>34</sup>, and the proposal for the Directive was opened upon and amended several times by different EU bodies,<sup>35</sup> no such second draft has been published so far.

Given the European Parliament vote on February 14, 2001, to endorse compromise amendments to the Copyright Directive, which reflect the balance of interests in the Council's common position on the adoption of the Copyright Directive (the "Common Position"),<sup>36</sup> a new draft should be available soon.

The proposed provisions regarding the protection of technological measures and rights management information are not provisions of material copyright law, but "flanking" measures for the enforcement of the copyright and neighboring rights law.

Although this is not a part of the implementation of the WIPO Treaties, it should be mentioned that Germany has not yet implemented the EU Directive on the Legal Protection of Services Based on, or Consisting of, Conditional Access (the "Conditional Access Directive").<sup>37</sup> The prescribed implementation date was May 28, 2000.<sup>38</sup> Art. 4 of the Conditional Access Directive requires Member States to prohibit, among others, the manufacture, import, distribution, sale, rental or possession for commercial purposes as well as the installation, maintenance or replacement for commercial purposes of illicit devices. Illicit devices are defined as devices that give access to a protected service in an intelligible form without authorization of the service provider.<sup>39</sup> In its official answer of October 6, 2000, to a reminder of the European Commission dated August 8, 2000, Germany pointed to the Council of Europe where the consultations with regard to a European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access were still under way.<sup>40</sup> Now that the European Access Convention has been adopted and opened for signature since January 24, 2001,<sup>41</sup> implementing legisla-

---

<sup>32</sup> See Bundesministerium der Justiz, *Diskussionsentwurf eines Fünften Gesetzes zur Änderung des Urheberrechtsgesetzes* [German Federal Ministry of Justice, Discussion Draft of a Fifth Amendment Act of the Copyright Act], July 7, 1998.

<sup>33</sup> COM(1997)628 final – 1997/0359 (COD), OJ C 108, 7.4.1998, p.8.

<sup>34</sup> See Herta Däubler-Gmelin, *Urheberrechtspolitik in der 14. Legislaturperiode – Ausgangspunkt und Zielsetzung* [Copyright Policy in the 14<sup>th</sup> Session of Legislature – Starting Point and Goals], ZEITSCHRIFT FÜR URHEBER- UND MEDIENRECHT ("ZUM") 43 (1999), 265 (271).

<sup>35</sup> See Opinion of the Economic and Social Committee of Sept. 9, 1998, OJ C 407, 28.12.1998, p. 30; Opinion of the European Parliament of Feb. 10, 1999, OJ C 150, 28.5.1999, p. 171; Amended Proposal of the Commission of May 21, 1999, OJ C 180, 25.6.1999, p.6; Common Position of the Council of Sept. 14, 2000 (visited Feb. 26, 2001) <[http://europa.eu.int/comm/internal\\_market/en/intprop/intprop/news/index.htm](http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/index.htm)>.; Communication from the Commission to the European Parliament of Oct. 20, 2000 (visited Feb. 26, 2001) <[http://europa.eu.int/comm/internal\\_market/en/intprop/intprop/news/index.htm](http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/index.htm)>.

<sup>36</sup> See European Commission, *Commissioner Bolkestein welcomes European Parliament vote on Copyright Directive* (visited Feb. 26, 2001) <[http://europa.eu.int/comm/internal\\_market/en/intprop/intprop/news/01-210.htm](http://europa.eu.int/comm/internal_market/en/intprop/intprop/news/01-210.htm)>. The Parliament's vote should help to ensure the Copyright Directive's rapid adoption.

<sup>37</sup> Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the Legal Protection of Services Based on, or Consisting of, Conditional Access, OJ 1998 L 320/54.

<sup>38</sup> Art. 6(1) of the Conditional Access Directive.

<sup>39</sup> Art. 2 lit. e of the Conditional Access Directive.

<sup>40</sup> Mitteilung der Bundesrepublik Deutschland an die Kommission der Europäischen Union vom 06.10.2000 [Communication of the Federal Republic of Germany to the Commission of the European Union of October 6, 2000] (visited Feb. 26, 2001) <<http://www.sicherheit-im-internet.de/download/012.htm>>.

<sup>41</sup> Council of Europe, *European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access*, European Treaties Series ("ETS") no. 178 (visited Feb. 26, 2001) <<http://conventions.coe.int/treaty/EN/cadreprincipal.htm>>.

tion should be available soon.

2.2. *Is your country active in the field of research concerning or development of technological measures?*

In 1995, the Fraunhofer Institute for Integrated Circuits (*Fraunhofer Institut für Integrierte Schaltungen*, the “Fraunhofer IIS-A”) in Nuremberg, devised one of the world’s first intellectual property protection schemes, the Multimedia Protection Protocol (MMP). This development was complemented in 1997 by the work on audio watermarking technologies. Ever since the announcement of the Secure Digital Music Initiative (SDMI) in December 1998,<sup>42</sup> Fraunhofer IIS-A has played a leading role in the development of the SDMI specifications. Besides working within SDMI, experts from the Fraunhofer IIS-A are involved in the MPEG-4 work on Intellectual Property Management & Protection and the AES activity on “Internet Audio Delivery Systems”.

The Fraunhofer Institute for Computer Graphics (*Fraunhofer Institut für Graphische Datenverarbeitung*) in Darmstadt, developed the Cryptographic Intellectual Property Rights Enforcement System (“CIPRESS”) on behalf of Mitsubishi Corporation in Tokyo, Japan.<sup>43</sup> CIPRESS is a system, which provides security mechanisms for both storage and network traffic in the digital domain, as well as a protection mechanism in the form of digital watermarking for the analog domain. Protection in the digital domain is achieved by enforcing mandatory encryption based inside the host operating system. The user has no influence over the fact that all data stored on the system (or remote file servers) is encrypted at all times. Similarly, transfers of data over networks are monitored, encrypted and decrypted on the fly without the possibility of user intervention.

2.3. *How does your legislation ensure the legal protection of technological measures?*

The discussion draft of an amendment to the German Copyright Act includes two separate provisions for the protection of technological protection measures and copyright management information in respect of all rights protected under the Act.

2.4. *Briefly describe the legislation.*

The § 96a UrhG draft introduces a prohibition of the circumvention, removal, destruction or otherwise means to render ineffective any technological measures that serve to protect against copyright or neighboring rights infringement:

*“Technological devices and measures, including computer programs, which serve to protect against an infringement of a right protected by this law may not be circumvented, removed, destroyed or otherwise rendered ineffective.”*

The right holder is not obligated to apply any technological measures. The § 96a UrhG draft applies only if such measures have in fact been taken.

While the expression “technological measures” is described in detail in Art. 6 (3), first sentence of the Common Position, the § 96a UrhG draft does not provide an equivalent legal definition.

The technological measures applied must serve to protect against an infringement of a right protected by the German Copyright Act, including the rights of the manufacturer of a computer program pursuant to § 9a *et seq.* UrhG and the rights of the makers of databases pursuant to § 87a *et seq.* UrhG. This does not contradict the fact that pursuant to § 69f(2) UrhG, computer program manufacturers have a claim to the destruction of means that are designed solely to remove or circumvent technological measures protecting programs without permission. Pursuant to § 69a(4) UrhG, special provisions for computer programs shall not prejudice the applicability of other legal regulations in respect to computer programs.

---

<sup>42</sup> See SDMI, *Who We Are* (visited Feb. 26, 2001) <[http://www.sdmi.org/who\\_we\\_are.htm](http://www.sdmi.org/who_we_are.htm)>.

<sup>43</sup> Fraunhofer Institut für graphische Datenverarbeitung, *CIPRESS – Project Information Page* (visited Feb. 26, 2001) <<http://www.igd.fhg.de/igd-a8/projects/cipress/overview/index.html>>.

Of crucial importance is the objective purpose behind a technological measure, *i.e.*, its abstract suitability for preventing the infringement of a right. Consequently, the impairment of the integrity or operability of such a measure is also prohibited if carried out for one of the uses permitted pursuant to the exceptions and limitations set out in § 45 *et seq.* UrhG. The draft under debate thus calls for more than what is required by Arts. 11 WCT or 18 WPPT. These provisions only require the legal protection of technological measures to the extent that they limit such “acts in respect of their works, which are not permitted by the authors concerned or are not permitted by law”. How technological measures work is, however, independent of the existence of specific circumstances justifying certain uses. According to the German Federal Ministry of Justice, this calls for a linking of legal protection to the abstract suitability of technological measures for protecting against the infringement of a right which is also in the interest of the right holder. If one were to permit circumvention of technological measures for permitted uses, the right holders would also lose the protection against possible future acts of infringements.

Due to the objective purpose requirement, the area of protection provided for by the § 96a UrhG draft appears to be limited to technological measures controlling the use and integrity of protected works and performances. Measures that solely limit the access to such works and performances appear not to be included, as the German Copyright Act does not provide for any exclusive access rights.

However, this distinction remains questionable as access control measures can also serve to control use and integrity. In order to gain access to digital works or performances, one has to copy them temporarily to the RAM of a suitable device. Pursuant to § 69c no. 1 UrhG, temporarily copying computer programs is an exclusive right belonging to the right holder. According to the prevailing opinion in Germany, temporarily copying of other works or performances to a user’s RAM is, *de lege lata*, also an exclusive right belonging to the right holder pursuant to § 16 UrhG. Access control measures prevent such temporary copying. Therefore, they also constitute use and integrity control measures and should consequently be covered by the § 96a UrhG draft.

The § 96b UrhG draft deals with the protection of copyright management information. In so far as copyright management information forms an integral part of a technological measure, technological measures should also be protected under this provision. Sec. 96b(1) and (2) UrhG draft read as follows:

*“(1) Copyright management information which is incorporated into the original or a copy of a work or a database or into a video or audio recording, or which is used in connection with the public communication of a work, a database or a video or audio recording may not be removed or manipulated without the permission of the right holder.”*

*“(2) Originals or copies of a work or a database or of a video or audio recording in respect of which copyright management information has been illegally removed or manipulated may not be disseminated or used for public communication.”*

The term “copyright management information” is defined in § 96b(3) draft UrhG as follows:

*“Copyright management information within the context of this law shall mean data containing information which serves to identify the object or the holder in respect of any of the rights protected under this law or the holder of a user right to such object or which is related to the conditions under which a user right is granted in respect of such object.”*

2.5. *List the sanctions available for violations and specify whether or not your country’s legislation provides for criminal sanctions.*

Secs. 96a and 96b UrhG draft are so-called protective laws (*Schutzgesetze*) in the meaning of § 823(2) of the German Civil Code (*Bürgerliches Gesetzbuch*, the “BGB”). Thus, any unlawful infringement entitles the right holders, whose works or performances are protected by the circumvented technological measure, to seek injunctive relief and to seek damages in cases of willful infringement.

Moreover, the discussion draft proposes to amend the existing § 99 UrhG as follows:

*“The provisions set forth in § 98 shall apply mutatis mutandis to devices that are the property of the infringer and are used or intended exclusively or almost exclusively for the manufac-*

*ture of copies or for the illegal removal, destruction, other act rendering ineffective or circumventing of technological means within the meaning of § 96a or for the illegal removal or manipulation of copyright management information.”*

Thus, the right holders may require that any such devices be surrendered to them in return for equitable remuneration, which may not exceed the cost of manufacture. Where this would lead to disproportionate results for the infringer, and if the illegal features of the devices can be eliminated in some other way, the right holders may claim only the measures necessary for such purpose.

Based on the discussion draft, whether all these claims extend to the producers of the circumvented technological measures remains unclear.

Neither the discussion draft nor existing legislation in Germany provide for specific criminal sanctions for the circumvention of technological devices applied to works or performances protected under the German Copyright Act.

2.6. *Which persons would be liable?*

*Those who engage in the act of circumvention?*

*Those who enable or facilitate the commission of an act of circumvention by*

- a. Supplying information?*
- b. Supplying devices?*
- c. Offering services?*

*Is knowledge or intent to circumvent a technical device a prerequisite for liability?*

The § 96a UrhG draft is limited to the act of circumvention. Sec. 96b(1) UrhG draft prohibits the removal and manipulation of copyright management information, and § 96b(2) UrhG draft disallows the dissemination or use of works, databases and recordings for public communication in respect of which copyright management information has been illegally removed or manipulated. Sec. 99 is directed against certain unlawful devices, which are the property of the infringer. Those who enable or facilitate the commission by supplying information and devices or offering services may be held liable for contributory infringement. The limitations on this doctrine in the field of copyright law, resulting from the exceptions to the exclusive rights, do not appear to apply to the draft anti-circumvention provisions.

Neither knowledge nor intent to circumvent are a prerequisite to liability under §§ 96a or 96b UrhG draft.

2.7. *Are there differences in the scope of the prohibition depending on the kind of technological measure circumvented? For example, is the prohibition the same with respect to: access controls; measures protecting rights of the copyright owner; copyright management information? If so, why?*

The discussion draft does not address the question why § 96b UrhG draft prohibits the dissemination or use of works, databases and recordings for public communication in respect of which copyright management information has been illegally removed or manipulated, whereas § 96a UrhG draft does not provide for a similar prohibition if a technological device has been removed.

2.8. *If supplying devices for circumvention is a prohibited act:*

- a. Does the definition encompass software (computer software)?*

The § 96a UrhG draft expressly provides for technological devices and measures to include computer programs.

- b. Does liability depend on whether the device is “effective”? If so, what standard is used to determine the effectiveness of a device?*

Sec. § 96a UrhG draft does not expressly call for the technological means being used to be “effective”. This is likely to be traced back to the fact that this adjective was not contained in Art. 6(1) of the initial proposal of the Copyright Directive. The standard thus deviates from Arts. 11 WCT and 18 WPPT and from Art. 6(1) of the Common Position. A serious effort should, however, be a prerequisite for the protection pursuant to § 96a UrhG draft. One could assume such a requirement to be a criterion for use

of the term “technological devices and measures”. However, a corresponding amendment of the draft would seem prudent.

- c. *How does the legislation take account of the fact that some devices capable of circumventing technological protection measures also have other, beneficial purposes? For example, does liability depend on whether circumvention is the “sole purpose” of the device, or its “primary purpose”, or on whether there are “commercially significant” uses for the device other than circumvention, or some other standard?*

The § 99 UrhG draft is limited to devices that are used or intended exclusively or almost exclusively for illegal purposes.

### **III. Exemptions to prohibitions; authorized circumventions.**

3.1. *Does your country’s legislation provide for exceptions to the prohibition on circumvention? Do the exceptions differ according to the type of measure at issue (access controls; measures protecting rights of the copyright owner; copyright management information)?*

*Exceptions for the benefit of users:*

*Do they correspond to all copyright exceptions?*

*Do they correspond to only some of the exceptions (e.g. draft EU Directive, seven listed exceptions)?*

*Is there a closed list of exceptions, or general criteria to assess the appropriateness of the exception?*

*Describe the circumvention exceptions under your country’s law.*

*What are the justifications for the exceptions for which your country’s legislation provides?*

*Are there new exceptions for circumvention of technological measures that did not expressly exist in your country’s prior copyright law?*

*Do exceptions differ depending on the type of technological means circumvented? Why?*

According to the § 96aUrhG draft, the holder of rights to works, databases or performances that are protected by technological measures may permit their circumvention. Such technological measures serve solely to protect their rights. If works or performances of various right holders are protected by the same technological measure, the permission of all of the right holders concerned – as in the case of § 69f(2) UrhG – must be obtained. In the case of co-authors, the second sentence of § 8(2) UrhG should apply by analogy. The § 96b UrhG draft allows for the removal or manipulation of copyright management information only with the permission of the right holder. Neither § 96a nor § 96b UrhG draft provide for any other exceptions.

3.2. *Does your country afford users the means to exercise the exceptions to circumvention? If so, how?*

Although Art. 6(4) of the Common Position obliges the Member States, in the absence of voluntary measures taken by right holders, to ensure that right holders make available to the beneficiary of certain exceptions or limitations provided for in national law the means of benefiting from those exceptions or limitations under certain circumstances, the German discussion draft does not contain any such obligation. However, a future implementation of the Copyright Directive in Germany will have to take this point into account.

3.3. *Are there private agreements (contracts, collective bargaining, etc.) that permit certain categories of users (e.g., public libraries) to circumvent? If so, why?*

No.

3.4. *Does your country’s legislation offset any circumvention exceptions with rights to remuneration or compensation?*

No.

3.5. *Do consumer equipment manufacturers have any obligation to design their products to recognize and comply with specific protection measures? Does your country's legislation address this issue, and if so, how?*

There are no such statutory obligations in Germany.

3.6. *What has been your experience under your country's legislation to date (e.g. court proceedings, administrative interpretation, etc.)?*

Not applicable.

3.7. *To what extent are works currently marketed in your country with technological protection? Please describe with as much detail as possible the kinds of works currently protected and the kinds of technological measures used.*

Technological protection devices such as hardware locks appear to be quite popular in the field of high-end computer programs in Germany. Most mass-market software is distributed without copy protection as widespread distribution appears to be key for the economic success of such software. Moreover, in the case of computer software, copy protection measures are not seen as important since other revenue streams such as maintenance and update fees complement the proceeds derived from the sale of licenses.<sup>44</sup>

In the field of audio CDs, a number of tests have been conducted in Germany. For example, BMG used the Cactus Data Shield, developed by the Israeli company Midbar,<sup>45</sup> for HIM's album *Razorblade Romance*. When audio CDs are produced, Cactus Data Shield is a mere one station, automatic device installed in-line between the data processing station and the mastering system, which does not require any changes to the production machinery or the pre-mastering system. It modifies the directory of the CD and creates "holes" in the data that leave an audio CD player unaffected but prevent a conventional CD-ROM player from playing the CD due to the latter's inability to bridge the gaps by interpolating the missing data. Sony tested SecuROM, a similar protective system,<sup>46</sup> at the beginning of the year 2000 with the album *Techno Club Vol. 9*. Unlike other systems on the market, SecuROM does not employ unreadable sectors (C2 errors) on the disc to create an electronic keycode. Rather, its digital signature offers a high compatibility rate (> 99.9 %) with all CD-ROM and DVD-ROM drives on the market, while preventing casual consumer copying and professional piracy.

For online audio distribution over the Internet, several different technological protection systems are currently being used in Germany:

One example is Deutsche Telekom's service "music on demand" (mod).<sup>47</sup> Users may choose from 70,000 different tracks. The music is then distributed in MPEG 1 Audio Layer 3 (MP3) files over an ISDN or DSL Internet connection and charged to the users telephone bill.<sup>48</sup> Fraunhofer IIS-A's Multimedia Protection Protocol (MMP) protects these files. Thus, the user can play the music only on the personal mod-player software which must be downloaded from the mod-website. The files can be copied to a CD-R or CD-RW for storage purposes only. Ordinary audio CD players will not be able to play these storage CDs.

The first large download project of a phonogram producer in Germany is BMG's "musicdownload24".<sup>49</sup> The music is distributed in the newer MPEG Advanced Audio Coding (AAC) format. In order to be able to play the music, users must first download and install the proprietary Sonique player

---

<sup>44</sup> MICHAEL LEHMANN, *Le droit d'auteur et protections techniques – questionnaire allemand*, in COPYRIGHT IN CYBERSPACE 363, 366 (ALAI ed., 1997).

<sup>45</sup> Midbar Tech Ltd., *General Information* (visited Feb. 26, 2001) <<http://www.matimop.org.il/newrdinf/company/c3283.htm>>.

<sup>46</sup> See Sony DADC Austria AG, *SecuROM* (visited Feb. 26, 2001) <<http://www.securom.com>>.

<sup>47</sup> See <<http://www.audio-on-demand.de>> (visited Feb.26, 2001).

<sup>48</sup> See MOD-Handbuch (visited Feb. 26, 2001) <<https://www.audio-on-demand.de/mod/home.htm>>.

<sup>49</sup> See <<http://www.musicdownload24.de>> (visited Feb.26, 2001).

and InterRights Point (IRP) software which decodes the music files. IRP is a digital rights management (DRM) technology developed by Intertrust Technologies Corporation.<sup>50</sup> After installation of the required software, musicdownload24 users must set up a clearing house account. The clearing house administers the users' rights via the IRP. Users may download and play songs until the credit in the IRP on their PC is used up. Then they need to contact the clearing house online in order to purchase further credit. Payment for this credit is made by direct debit from the users' respective bank accounts.

Other DRM systems for online distribution include Liquid Audio,<sup>51</sup> Microsoft Windows Media Rights Manager<sup>52</sup> and IBM Electronic Media Management System.<sup>53</sup>

---

<sup>50</sup> See Intertrust, *InterTrust Technology* (visited Feb. 26, 2001) <<http://www.intertrust.com/main/technology/index.html>>. There are four primary architectural elements in the InterTrust DRM platform:

1. The core element of the InterTrust architecture is the IRP, which operates on the users' PCs. Each IRP creates a local, secure database that stores the users' rights, identities, transactions, budgets, and keys.
2. Information in the InterTrust system is encrypted and stored in a DigiBox container. Once in a DigiBox container, the information can flow across unsecured networks, and only an IRP satisfying the required rules can access and process these files. Information in a DigiBox container remains protected even after a user has accessed it, providing persistent protection of the information and continuing control over its use, regardless of where the information travels.
3. Content usage is managed by rules, including price, payment offer, play, view, print, copy, save, superdistribution. InterTrust provides a variety of tools for allowing providers to create and change rules, and associate them with digital information. Rules are protected in the same way content is protected. Rules can travel with the information, or separately, allowing InterTrust partners the flexibility to change any rule, including rights or price, after content has been delivered. IRPs ensure that applicable rules are followed every time an information usage "event" is requested.
4. IRPs connect to InterTrust processing partners' data centers through a communications controller system called the Transaction Authority Framework. The Transaction Authority Framework collects transaction records from IRPs, stores the records, and forwards them, as specified by usage rules, for further processing, including payment fulfillment. The Transaction Authority Framework also stores messages resulting from this further processing, such as payment confirmation, and when the IRP next connects to the data center, sends these messages to the IRPs. The Transaction Authority Framework includes administrative software called the Deployment Manager, which activates IRPs and manages them after activation, including fraud detection, revocation, security updates, and backup services.

<sup>51</sup> See <<http://www.liquidaudio.com>> (visited Feb. 26, 2001).

<sup>52</sup> See <<http://www.microsoft.com/Windows/windowsmedia/en/wm7/drm.asp>> (visited Feb. 26, 2001).

<sup>53</sup> See <<http://www.ibm.com/software/emms>> (visited Feb. 26, 2001).