ALAI 2001 National Report
Session IC
Finland

Prepared by Ms. Katariina Sorvari, Research Assistant, LL.Lic.; University of Turku and Ms. Tiina Ryhänen, IPR Manager, LLM, Radiolinja

ALAI 2001 Congress, New York, June 13-17:

Adjuncts and Alternatives to Copyright

Session I.C.

Situating legal protections for copyright-related technological measures in the broader legal landscape: ANTI CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT

Questionnaire prepared by Séverine Dusollier, Facultés Universitaires Notre-Dame de la Paix, Namur, Belgium

Preliminary comment

Following the adoption of the WIPO Copyright Treaty, and notably its article 11, several countries have enacted, or are in the process of enacting, provisions in the copyright regulatory framework that would prohibit the circumvention of technological measures protecting access to or rights in copyrighted works, and/or the distribution of devices enabling such circumvention.

Circumventing technological protection measures is not unprecedented. Precedents of anti-circumvention provisions are to be found in other fields of law, such as broadcasting law or provisions against computer crime. The rationales behind these provisions are quite different from copyright, however. They vary from safeguarding the confidentiality of the communication, to protection of the remuneration for the service, or the security of the network or computer processing system. In addition to these specific claims, general tort or unfair competition laws might also help prohibit any disabling or defeating of a technical fence.

Questions 1-9 of this Questionnaire inquire into the legal tools, *outside the copyright framework*, that prohibit or penalize:

- the defeating, circumvention or decryption of a technological measure;
- the private or commercial activities related to devices enabling or facilitating circumvention (preparatory acts); or
- the unauthorized reception, interception of or unauthorized access to technologically protected content.

The final question (10), inquires whether these extra-copyright measures could nonetheless be applied to protect against the circumvention of technological measures used in connection with copyrighted works. (For example, would these laws suffice to protect against the circumvention of copyrighted works, without the enactment of additional, copyright-specific laws?)

Questionnaire:

PLEASE APPEND STATUTORY TEXT AND GIVE CITATIONS TO COURT DECISIONS WHERE RELEVANT

We would be grateful if those national reporters who can answer the questionnaire in both French and English would do so.

1. Types of Circumvention

Are any of the following acts prohibited under some legal regime in your country, and if so, please specify which regime:

a. Gaining access

- to a technologically protected computer system …

Yes; Penal Code Chapter 38, Section 8: *Computer break-in* (578/1995)
(1) A person who by using an unauthorised access code or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most one year.
(2) A person shall also be sentenced for a computer break-in if he, without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system referred to in (1).
(3) An attempt is punishable.
(4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

- … or to protected material without authorization?

Yes; Telecommunications Market Act (396/1997)
Section 25:
Decoding systems. Unlawful possession, use, manufacture, import, marketing and sales promotion of a decoding system of a protective code shall be forbidden.
Section 45:
Anyone who willfully: - -
5) holds, manufactures, uses, imports or markets a decoding system or promotes its sales in violation of section 25 shall, if a more severe penalty is not provided for elsewhere in the law, be sentenced for a violation of the provisions on telecommunications operations to a fine.

b. Receiving protected data or material without authorization or without paying the due remuneration?

No; if reception requires simultaneously unlawful decoding, gaining access to protected material is prohibited as above mentioned.

c. Gaining access to a technologically protected computer system or to protected material by supplying a false name or password?

Yes, see a.1. and a.2.

d. Gaining access to a technologically protected computer system or to protected material by supplying a false Internet protocol (i.p.) address?

Not specifically mentioned in legislation, yes, if complies with the paragraphs mentioned above in sections a.1. and a.2.

e. Gaining access to technologically protected material by supplying false payment information?

Yes, under general principles of fraud and means of payment fraud.
Penal Code Chapter 36 Section 1: *Fraud* (769/1990)
(1) A person who, in order to obtain unlawful financial benefit for himself/herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for *fraud* to a fine or to imprisonment for at most two years.
(2) A person who, with the intention referred to in (1), by entering false data into a computer or by otherwise interfering with automatic data processing, falsifies the end result of data processing and in this way causes another person economic loss shall also be sentenced for fraud.
(3) An attempt is punishable.

Penal Code Chapter 37 Section 8: *Means of payment fraud* (769/1990)
(1) A person who, in order to obtain unjustified economic benefit for himself/herself or another
1) uses a means of payment without the permission of the lawful holder, in excess of his/her right based on such permission, or otherwise without lawful right, or
2) transfers such a means of payment or means of payment form to another in order to have it used without lawful right shall be sentenced for *means of payment fraud* to a fine or to imprisonment for at most two years. (602/1997)
(2) Also a person who, by overdrawing his/her account or exceeding the agreed maximum credit limit, misuses a means of payment referred to in paragraph (1) and in this way causes economic loss to another shall be sentenced for means of payment fraud, unless when using the means of payment he/she intended to compensate the loss without delay.

f. Decrypting without authorization encrypted content?

Yes, see above a.2.

g. Overriding a limit on the number of simultaneous users allowed access or on the allowed time of access?

Not specifically mentioned in the legislation; general principles of e.g. unauthorized use apply.
Penal Code Chapter 28 Section 7: *Unauthorised use* (769/1990)
(1) A person who unjustifiably uses the movable property or the non-movable machine or equipment of another shall be sentenced for *unauthorised use* to a fine or to imprisonment for at most one year.
(2) An attempt is punishable.

h. Overriding a limit on the number of copies an authorized user is permitted to make, or a technologically enforced prohibition against making *any* copies?

Not specifically mentioned in the legislation; general principles of copyright law apply
Penal Code Section 1: *Copyright offence* (1010/1995)
(1) A person who for profit and in violation of the Copyright Act (404/1961) and in a manner conducive to causing considerable inconvenience or damage to the rightholder, breaches the right of another to
1) a literary or artistic work;
2) the performance of a literary or artistic work;
3) a record or other device where sound has been recorded;
4) a film or other device where moving images have been recorded;
5) a television or radio broadcast;
6) a register, table, program or another similar work referred to in the Copyright Act and containing the compilation of a lot of information, or a database whose compilation, verification or presentation has required a lot of effort; or (251/1998)
7) a photograph
shall be sentenced for a *copyright offence* to a fine or to imprisonment for at most two years.

Copyright Act Section 56a (442/84):
Anyone who
1) willfully or out of gross negligence violates a provision issued for the protection of copyright in the present Act or acts in violation of an instruction issued under Article 41, second paragragh, of a provision of Article 51 or 52, or of a prohibition referredto in Article 53, first paragraph, or Article 54b; or
2) - -
shall, unless the act is punishable as a copyright crime under Article 1 of Chapter 49 of the Penal Code, be sentenced for a copyright offence to a fine.

2. General tort law rules of direct or secondary liability:

a. Under your country's general tort law principles, could a person be held liable for having engaged in an act of circumvention or for having manufactured or distributed a circumvention device? What would be the conditions for liability?

Mere circumvention or distribution of a circumvention device does not create civil liability; any financial damages must however be compensated under the general principles of tort law: anyone who willfully or out of negligence causes someone damages is liable to compensate these damages.

b. Has your country's case law already applied tort law to prohibit or to enjoin the act of circumventing or the manufacture or distribution of a circumvention device? Are knowledge or intent required? How have knowledge or intent been defined? Is the liability of manufacturers and distributors of devices direct, or based on secondary liability (contributory or vicarious)?

No precedents in the Supreme Court.

c. If general tort principles may apply in your country to prevent the act of circumventing, or the supplying of circumvention devices, are there exceptions to the scope of the prohibitions?

None.

d. Under what circumstances might resort to technological measures to block access be considered in your country an "abuse of right"?

No legislation or case law.

3. Broadcasting law, cable and satellite regulations, protection of encrypted services or broadcasts, protection of conditional access services

a. Are encrypted services or broadcasts (e.g. pay-TV signals, etc.) legally protected in your country? Is the regulation civil, administrative, criminal or public? What is the rationale for this regulation?

Yes, the regulation is civil, i.e. telecommunications legislation. The rationale for the regulations is to protect encrypted services and broadcasts against the unauthorized use.

b. In such legislation, is the decryption, descrambling or any other form of unauthorized interception of encrypted services or broadcasts prohibited? Under what conditions? What are the rationale and purpose for such prohibition? What are the services or programs at issue? Is protection available only if the broadcast or transmission requires payment? (i.e., no protection for free broadcasts of transmissions?) Who may bring a claim? What remedies are available?

Yes, unauthorized decryption of encrypted services and broadcasts is prohibited provided that the decryption is done by an equipment, part of equipment or another system whose purpose is to

decode the protective code effected through specific technical means from a message conveyed in the telecommunications network (Section 4 and 25 of Telecommunications Market Act). For rationale and purpose see Point 3a above. The services at issue are any technically protected messages conveyed in the telecommunications networks, including cable and satellite broadcasts. The protection is not limited to broadcasts or transmissions requiring payment. Also free broadcasts and transmissions are covered. The claim may be brought by an injured party or a public prosecutor. The remedies that are available include criminal and civil law sanctions.

c. Is the distribution of devices that enable or facilitate circumvention illicit? What are the criteria for considering a device to be illicit? For example, is there a requirement of knowledge or intent to engage in or facilitate illicit circumvention? What commercial/private activities related to that device are prohibited (manufacture, distribution, sale, possession, etc…)? How does the law address devices that potentially have licit and illicit purposes? Who may bring a claim? What remedies are available?

Yes, distribution of unauthorized devices is illicit. Any unauthorized decoding systems (for definition for decoding system see Point 3b above) is considered to be illicit provided that there is knowledge of such circumstances. According to Section 25 of the Telecommunications Market Act unlawful possession, use, manufacture, import, marketing and sales promotion of a decoding system of a protective code is forbidden. The provision prohibits both commercial and private activities. The claim may be brought by an injured party or a public prosecutor. The remedies that are available include criminal and civil law sanctions.

d. Are there circumstances in which circumvention or decryption is authorized or exempted from the prohibition? How have courts in your country applied the prohibitions (or exceptions) to circumventing technological protections for broadcasts and transmissions?

The Telecommunications Administration Centre may grant permission for the use of a decoding system. There are several decisions of Courts of First Instance on unauthorized decoding devices used for encrypted satellite and cable broadcasts.

e. Do you consider these legal provisions as adequate and effective?

The legal provisions in force are not considered to be adequate and effective enough. Government proposal amending these regulations is pending in the Parliament.

f. Conditional Access:

In The European Union, a directive of 1997 protects conditional access services, defined as "services provided against remuneration and on the basis of conditional access," whereas "Conditional Access" means "*any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon prior individual authorization."* Protected services could be television and radio broadcasting services as well as Information Society Services, e.g. video or audio-on-demand, electronic publishing, on-line access to a database and a wide range or other on-line services.

1. Is there a similar protection in your country? In which legal regime (broadcasting law or other)?

   Yes, in telecommunications legislation. See Point 3 above.

2. If yes, what is the rationale of the protection? Which services are covered? What are the requirements for protection? Is conditional access defined on the basis of a requirement of payment for the transmission? Is the circumvention of the conditional access measure and/or the circumvention device prohibited? Which activities related to circumvention devices are prohibited (sale, manufacture, possession, etc.)?

   See Point 3 above. Furthermore, the Government proposal implementing the Directive is pending in the Parliament.

3. The European Directive also covers the so-called "Information Society services", i.e. services provided at distance upon individual request from the recipient of the service. Does your legislation on conditional access concern information society services as well? In other words, could your conditional access legislation be applied to services provided through the Internet or other networks?

   Yes, see Point 3 above.

4. Telecommunications Law:

   a. Telecommunications law sometimes prohibits unauthorized interception of any wire or electronic communication. This could serve as a basis for a claim against decryption or any other unauthorized means of getting access to data when transmitted over telecommunication networks. Does your country's telecommunications law include such a prohibition?

      Yes.

      If so,

      1. Which acts are concerned (interception, disclosure, unauthorized access, reception, etc.)? Does the law cover interception devices as well?

         According to Section 4 of Act on the Protection of Privacy and Data Security in Telecommunications no one who has received or otherwise learned of a confidential telecommunications message not meant for him may, without justification, disclose the contents of the telecommunications message or make use of his knowledge of the contents or existence of the telecommunications message. For devices see Point 3 above.

      2. Does the content have to be encrypted or otherwise protected so as to benefit from protection?

         No, according to Section 4 of Act on the Protection of Privacy and Data Security in Telecommunications all telecommunications messages are confidental unless they are meant to be received by the public, i.e. the content does not have to be encrypted in order to benefit from the protection.

      3. What are the circumstances where interception is authorized or where interception devices are legitimate (e.g., when they comply with some technical standards)?

         Interception is authorized if the telecommunications message is meant to be received by that person. Access to the encrypted services is authorized, when a service provider has given its consent to the use of its services. The devices are legitimate if the service provider has authorized the use of decrypting devices or the Telecommunications Administration Centre has granted a permission for a use of such device.

      4. Who may bring a claim? What remedies are available?

         An injured party or a public prosecutor. Criminal and civil law remedies.

   b. Telecommunications law might also impose mandatory technical standards to be applied to telecommunication reception devices. This could lead to prohibiting devices enabling the unauthorized reception of communications. What about the telecommunications law in your country?

      No.

5. Computer crime

a. In your country, is there legislation related to computer crime? Can circumvention of technological measures and/or unauthorized access to computer systems, networks or data be prosecuted under such statutes? What is the rationale of criminalizing such offenses?

Yes, Chapter 38 of the Penal Code contains provisions on data and communications offences. According to Section 8 it is illegal to use an unauthorized access code or otherwise break a protection in order to unlawfully hack into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner. Furthermore, according to Section 8 it is illegal without hacking into the computer system, use a special technical device to obtain information contained in a computer system. The rationale of these provisions is to protect the computer systems against an unauthorized access.

b. What is the definition of the offense? Is the way of getting unauthorized access defined : e.g. providing a false password, decrypting, cracking the technical protection, etc.?

See Point 5 a above.

c. Can the manufacture or distribution of devices enabling the carrying out of these offenses be prosecuted as well (such devices are sometimes called 'hacker tools')? If not, could the seller or manufacturer of circumvention devices be prosecuted as an accomplice? What are the penalties for the offense?

No, the manufacture or distribution of devices cannot be prosecuted under Section 8. The penalties are a fine or imprisonment for at most one year. Futhermore, an attempt is punishable.

d. Is knowledge or malicious intent required to constitute the violation?

Knowledge is required.

e. Has computer crime legislation already been applied by your country's courts to the unauthorized access to protected information or transmissions, or to the circumvention of technological protection measures?

There is a case pending at the Court of First Instance.

f. In the absence of specific provisions on computer crime, could unauthorized access and/or the circumvention of technological measures be considered to violate other penal laws (e.g., offences such as theft, fraud, breaking and entering, forgery, etc.)? Are there some examples in the case law?

Yes, e.g. fraud or unauthorized use. There are examples in the case law, i.e. decisions of Courts of First Instance.

6 Unfair Competition law or unfair commercial practices

a. In your country, in the absence of specific prohibitions on circumvention or unauthorized access, has the distribution of circumvention devices or descramblers been prohibited through the application of unfair competition law? Under what circumstances?

No.

b. What are the advantages, disadvantages and boundaries of the recourse to unfair competition law as far as circumvention activities or devices are concerned? Do you consider this protection as sufficient and effective?

Because circumvention is mentioned in the Telecommunications Market Act, this discussion is not relevant in Finland.

7. Protection of technological measures as such

Technical means of protection might be in themselves protected by a proprietary right, e.g. by a copyright (for instance if the technological measure consists of software), patent or trade secrets. In such a case, circumventing the software or the technical system or developing circumvention devices could effect an unauthorized reproduction of the software (namely by reverse engineering) or a disclosure of the trade secret.

a. In your country, what legal regime of exclusive or related rights might apply to the technological measure? Under what conditions? Do you know any case law in that field?

General principles of all intellectual property rights apply; no case law.

b. What exceptions related to these legal regimes could be applied to legitimate the circumvention act or device?

Circumvention as such is not an infringement of an intellectual property right (with the possible exception to copyright to computer programs and databases) and therefore all exceptions may apply.

8 Other protections

a. Can you think of any other means of protecting technological measures against circumvention in your country? In which legal areas and by which mechanisms (e.g., privacy law, property right, "trespass", “conversion,”…)?

No.

b. In particular, do you think that, in your country, contract law can offer an effective prohibition against circumvention?

Contract law is not a sufficient tool for protecting rightholders from circumvention. It is a good addition to other legal protection but e.g. the needs of third parties require an effective prohibition legislation apart from contract law.

1. For example, a contract obliging each user not to circumvent can be embedded in the technological measure itself when it enables the on-line licensing of or access to transmissions (including content). Would such a contract be enforceable in your country?

Enforceability of such a contract is questionable especially in consumer contracts

2. Or contracts might be negotiated between content providers and the computer or consumer electronic manufacture industries in order to oblige them either to design devices that answer to technological measures or not to develop devices that are able to circumvent them. Are such negotiations in progress in your country?

No.

9 Limitations, exceptions, fundamental rights, third parties' and public interest

a. Are there any general limiting principles that could apply to the various legal regimes we have addressed in this report (e.g. freedom of expression, freedom of information, public interest, consumer protection, abuse of right, etc.)?

The main purpose of telecommunications legislation is to protect the confidentiality of telecommunications messages, i.e. the right that cannot be limited by principals such as freedom of information or consumer protection.

b. What are the concerns of computer and consumer electronics industries related to prohibitions of circumvention devices? Have these concerns been taken into account in the legal provisions addressed above?

In general, the related industries are concerned for a need of adequate protection against illegal decrypting devices. These concerns as well as concerns of service providers have been taken account in the telecommunications legislation.

10. Potential application of the protections surveyed in Questions 1-9 to copyrighted works

a. In your country, could copyright holders avail themselves of some or all of these extra-copyright legal provisions or mechanisms, either to prevent the act of circumvention of technological measures, or to prohibit trafficking in circumvention devices? If so, which ones?

In principal, copyright holders could directly benefit from protection against unauthorized decoding systems provided that a copyright holder is also a service provider.

b. Could the alternative means of protection for technological measures available in your country be added or used simultaneously with copyright-related anti-circumvention provisions?

Yes, the object of protection is different. Copyright-related technological measures protect content, i.e. copyrighted works, whereas telecommunications legislation protects services and service providers.

c. What would be the pros and cons of recourse to extra-copyright protections against circumvention of access to copyrighted works or circumvention of technological protections of rights of the author? Do these protections call for reassessment of the need for copyright-specific protections?

Extra-copyright protections indirectly protect against unauthorized access to copyrighted works, but they do not give adequate and direct protection to works or to technological measures against unauthorized access or circumvention. Therefore, copyright-specific protections are needed.

d. If recourse to extra-copyright protections is available, could your country implement the WIPO treaty obligations without copyright-specific anti-circumvention legislation? In your view, would this be a desirable approach? If not, to what discrepancies or failures in the existing law would copyright-related anti-circumvention provisions need to respond?

No, copyright-specific anti-circumvention legislation is needed. See Point 10 c above.

Any other observations?

No.