.[Translation]

Directions Defining the Content of the Subparagraphs of Paragraph 3 of Article 80-2 of the Copyright Act

Provisions	Comments
1. These Directions are pursuant to paragraph 4 of Article 80-2 of the Copyright Act (herein after referred to as "the Act").	These Directions are pursuant to paragraph 4 of Article 80-2 of the Copyright Act ("the Act") to elaborate the regulatory principles set out in paragraph 3 of Article 80-2 of the Act.
2. The terms "disarmed, destroyed, or by any other means circumvented" in paragraph 1 of Article 80-2 of the Act and "disarming, destroying, or circumventing" in paragraph 2 of the same article are referred to in these Directions by the abbreviated term "circumvent."	The term "circumvent" in these Directions means "disarm, destroy, or by any other means circumvent" referred to in paragraph 1 of Article 80-2 of the Act, and "disarming, destroying, or circumventing" referred to in paragraph 2 of the same article.
3. The equipment, devices, components, technology, or information listed below may not be manufactured, imported, offered to the public for use, or offered in services to the public, except in the circumstances set out in paragraph 3 of Article 80-2 of the Act: (1) That which is primarily for the purpose of circumventing a technological protection measure; (2) That which has limited commercial purpose other than the purpose in the preceding subparagraph; (3) That which is marketed for use in circumventing a technological protection measure	1. Under the principle of technological neutrality, equipment, devices, components, technology, or information for circumventing technological protection measures are not uniformly all prohibited from being manufactured, imported, offered to the public for use, or offered in services to the public. Only those meeting certain criteria are rated negatively and subject to restriction. Relevant conditions are therefore prescribed after having reference to the US, European, Japanese, Korean, and Hong Kong regimes and the content of relevant free trade agreements. 2. The term "technological protection measure" in these Directions encompasses both technological

Provisions	Comments
protection measure.	protection measures to prohibit or restrict access to works ("access controls") and technological protection measures to prohibit or restrict exploitation of works ("exploitation controls").
4. The circumstances in the preceding point are also prohibited with respect to components, parts, or products of electronics, communications, or computing products, provided that the person who is manufacturing them, importing them, offering them to the public for use, or offering them in services to the public shall not have any duty, in the design or selection of such products and components and parts thereof, of providing for a response to any particular technological protection measure.	1. Among its various functions, a multifunction electronic device may have a function that circumvents a technological protection measure, although the device is not designed primarily for purposes of such circumvention. Therefore, clarification is required as to whether manufacture and distribution of such devices would be prohibited under the Act's protections for technological measures. 2. The US Digital Millennium Copyright Act Section 1201(c)(3) states in part, "Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1)" [which corresponds to the prohibitions adopted in Point 3 regarding paragraph 3 of Article 80-2.].

Provisions	Comments
	Paragraph 48 of the preamble to the 2001 European Copyright Directive, states, "Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6" [which corresponds to the prohibitions adopted in Point 3 regarding paragraph 3 of Article 80-2.]. The intent of these provisions is to strike a balance between the interests of economic rights owners and the interests of manufacturers and sellers of multifunction electronic devices. Given the necessity of this, the above legislation was taken into reference in drafting the Directions.

Provisions	Comments
5. "To preserve national security" in subparagraph 1 of paragraph 3 of Article 80-2 of the Act means lawfully authorized activities to protect information security or intelligence and other related matters for preserving national security. "Information security" in the preceding paragraph means acts carried out for purposes of identifying and handling vulnerabilities in government-administered computers, computer systems, or computer networks.	1. This point applies to circumstances in which it is permissible to circumvent technological protection measures in lawfully authorized activities for purposes of preserving national security, including permissibly circumventing access controls, or manufacturing, importing, or providing equipment, devices, components, technology, or information for circumventing access or exploitation controls. 2. Examples: (1) To prevent invasions by hackers of government-administered computers, the Research, Development, and Evaluation Commission, Executive Yuan, may, itself or by outsourcing to contractors, carry out testing of computers administered by various government agencies, to identify or treat vulnerabilities in the computers and make improvements to safeguard information security. (2) To preserve national security, the National Security Bureau, upon identifying suspected threats to national intelligence needs, may disarm suspicious computers or servers, or technological protection measures attached to specific documents or files therein, to ascertain whether there is an intended threat to the country. 3. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(e) concerning exemption for lawfully authorized intelligence and other government activity.

Provisions	Comments
6. "Done by central or local government agencies" in subparagraph 2 of paragraph 3 of Article 80-2 of the Act means any lawfully authorized prosecutorial, investigative, or other government activity of a central or local government agency.	1. This point applies to circumstances in which a central or local government agency may circumvent technological protection measures in lawfully authorized government activities, including permissibly circumventing access controls, or manufacturing, importing, or providing equipment, devices, components, technology, or information for circumventing access or exploitation controls. 2. Example: A prosecutorial agency conducting an inquiry into a criminal offense under the Code of Criminal Procedure is exercising national public powers vested by the Code of Criminal Procedure or related special laws (e.g. the Communications Safeguards and Supervision Act), and so may circumvent technological protection measures for purposes of carrying out such lawfully authorized activities. 3. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(e) concerning exemption for lawfully authorized intelligence and other government activity.
7. "Done by file archive institutions, educational institutions, or public libraries to assess whether to acquire the information" in subparagraph 3 of paragraph 3 of Article 80-2 of the Act shall be subject to the following conditions:	1. This point applies to circumstances in which a file archive or other institution may circumvent access controls for purposes of assessing whether to acquire the information. 2. "File archive institutions, educational institutions, or public

Provisions	Comments
(1) An identical copy of the accessed work is not reasonably available in another form; (2) After accessing the work, it is not retained longer than necessary to make a good faith determination of whether to acquire the work, and is not used for any other purpose. An institution accessing a work in compliance with the preceding paragraph may circumvent a technological protection measure prohibiting or restricting access to the work.	libraries" in this Point refers to those that are nonprofit, and whose collections are open to the public, or though not open to the public are available to researchers of the archives, educational institution, or library, and departments of its affiliated organizations and to other persons doing research in a specialized field. 3. Examples: (1) A certain publisher publishes an electronic encyclopedia, but there is no trial-use version, and a copy of the work is not reasonably available in any other form (e.g. a paper version), necessitating that a library buy the electronic version in order to ascertain and assess whether the content of the encyclopedia is worth buying. In these circumstances, if the electronic encyclopedia has access controls so that the library is unable to access the content of the work before actually buying it, for purposes of ascertaining and assessing whether the work is worth buying for its collection, it is permitted to access and examine the work after circumventing the controls for purposes of assessing whether to buy it, so as to avoid nonprofit archives, educational institutions, or public libraries wasting funds on the purchase of unneeded materials, thus balancing public and private interests. (2) The mechanical engineering department of a certain university wishes to assess whether certain

Provisions	Comments
	software meets its needs for procurement purposes, but the manufacturer of the software has not provided a reasonable means of assessment and employs access controls. To prevent the university from buying software that does not meet its needs, it is permitted to access and examine it after circumventing the controls, to assess whether to buy it, thus balancing public and private interests. 4. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(d) concerning exemption for nonprofit libraries, archives, and educational institutions.
8. "To protect minors" in subparagraph 4 of paragraph 3 of Article 80-2 of the Act shall be subject to the following conditions: (1) It prevents the access of minors to works on the Internet; (2) It does not violate the provisions of the Act.	1. This point applies to circumstances in which it is permissible to circumvent access controls for purposes of protecting minors. 2. Under the circumstances set out in this point, it is permissible to circumvent access controls, and to manufacture, import, or provide equipment, devices, components, technology, or information for circumventing access controls. 3. Example: There are certain works on the Internet with pornographic or violent content that are unsuitable for access and viewing by minors. From the standpoint of protecting minors, under the Child and Youth Welfare Act and related laws and regulations, a rating system should be adopted. However, if such works, or a server on which such works are stored, is protected by encryption or other

Provisions	Comments
	access controls, so that the content cannot be distinguished on a case-by-case basis, it becomes impossible to put ratings into practice to protect minors. For the purpose of protecting minors, it is therefore permissible to circumvent the technological protection measures. 4. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(h) concerning exemptions for protection of minors.
9. "To protect personal data" in subparagraph 5 of paragraph 3 of Article 80-2 of the Act refers to the following circumstances: (1) The technological protection measure or the work it protects has the capability of collecting or disseminating personal information reflecting the online activities of an individual natural person who seeks to gain access to the work; (2) In the normal course of its operation, the technological protection measure or the work it protects does not provide notice of the capability described in the preceding paragraph, and does not provide the option of preventing or restricting that function; (3) Circumvention has the sole effect of identifying and disabling the capability described in subparagraph (1), and has no other effect on the	1. This point applies to circumstances in which it is permissible to circumvent access controls to protect personal information. 2. Example: A certain work or a technological protection measure of the work has the capability of automatically collecting or disseminating information about the online activities of a person accessing the work. However, it fails to provide notice to the user, causing the user to unknowingly have personal information reflecting his or her online activities collected or disseminated, seriously violating the individual's right of privacy. To protect the individual right of privacy and balance the legal protection of technological protection measures, it is therefore permissible to circumvent technological protection measures under the circumstances set out in this point, to avoid such collection or dissemination functions. 3. This point is adopted with reference

Provisions	Comments
ability of any person to gain access to any work; (4) The purpose of circumvention is solely for the purpose of preventing the capability described in subparagraph (1), and the act of circumvention is not in violation of any other law or regulation. Where all the circumstances in the subparagraphs of the preceding paragraph are met, it is permissible to circumvent a technological protection measure prohibiting or restricting access to a work. Paragraph 1 does not apply to a technological protection measure, or a work it protects, that does not collect or disseminate personal information, or that is disclosed to a user as not having or using such collection or dissemination capability.	to the US Digital Millennium Copyright Act Section 1201(i) concerning exemption for protection of personally identifying information.
10. "To perform security testing of computers or networks" in subparagraph 6 of paragraph 3 of Article 80-2 of the Act means accessing a computer, computer system, or computer network, for the purpose of testing, inspecting, or correcting, a security flaw or vulnerability. The provisions of the preceding paragraph shall be subject to the following conditions:	1. This point applies to circumstances in which it is permissible to circumvent technological protection measures to perform security testing of computers or networks, including circumventing access controls, and developing, manufacturing, or employing equipment, components, or technology for circumventing access controls. 2. Example: To test whether the firewall of the website of a certain agency has an ...

Provisions	Comments
(1) The security testing is performed solely by the owner or operator of such computer, computer system, or computer network, or a person authorized thereby; (2) The information derived from the security testing information is used solely to promote the security of the owner or operator of such computer, computer system, or computer network, or shared directly with the developer of such computer, computer system, or computer network; (3) The information referred to in the preceding subparagraph was used or maintained in a manner that does not infringe copyright, nor does it include any violation of privacy, breach of security, computer crime, or violation of any other act or regulation. A person permitted to access a computer, computer system, or computer network in compliance with the preceding two paragraphs may circumvent a technological protection measure prohibiting or restricting access to a work, provided that the person's conduct does not infringe copyright or violate any applicable act or regulation. It is permissible to develop, manufacture, distribute, or employ equipment, devices, components, technology, or information for circumventing technological	website of a certain agency has any flaw or vulnerability, making it vulnerable to unauthorized hacking or invasion by others, it is permissible, for the sole purpose of security testing and where there is no violation of the Copyright Act or any other act or regulation, to circumvent a technological protection measure to access the computer, computer system, or computer network. This [point] is also applicable to developing, manufacturing, distributing, or employing, for the sole purpose of such security testing, equipment, devices, components, technology, or information for circumventing technological protection measures prohibiting or restricting access to works, or to firms providing such services. 3.This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(j) concerning exemption for security testing.

Provisions	Comments
protection measures prohibiting or restricting [access] to works for the sole purpose of performing security testing described in paragraph 1, provided that such equipment, devices, components, technology, or information do not violate Point 3.	
11. "To conduct encryption research" in subparagraph 7 of paragraph 3 of Article 80-2 of the Act means activities to identify and analyze flaws or vulnerability of encryption technologies applied to copyrighted works, where conducted for purposes of advancing encryption technology or developing encryption products, and where in compliance with the following conditions: (1) The person has lawfully obtained the encrypted copy or content of the published work; (2) The encryption research cannot be conducted without circumvention; (3) The person attempted to obtain authorization to circumvent from the rights owner before taking the action, but did not receive consent; (4) The act does not infringe copyright, nor does it include any violation of privacy, breach of security, computer crime, or violation of any other act or regulation	1. This point applies to circumstances in which it is permissible to circumvent technological protection measures to conduct encryption research, including circumventing access controls, and developing or employing equipment, components, or technology for circumventing access controls. 2. Example: Collecting and studying works on the market that have technological protection measures attached, and use encryption technology, for purposes of researching new encryption technology to develop new technological protection measures or new network security mechanisms. Such research activity is beneficial to the development of encryption technology, so circumvention of technological protection measures attached to lawfully acquired copies of works and works for which authorization has been sought but could not be obtained is permitted for the sole purpose of such encryption technology research, provided that it

Provisions	Comments
or regulation. In determining whether encryption research complies with the subparagraphs of the preceding paragraph, the following factors shall be considered: (1) Whether the information derived from the encryption research was disseminated; if so, whether it was disseminated in a manner to advance encryption technology; whether it was disseminated in a manner that infringes copyright, or includes any violation of privacy, breach of security, computer crime, or violation of any other act or regulation; (2) Whether the research purpose of the person conducting the encryption research is lawful; whether the person is employed by another person; whether the person is appropriately trained or experienced; (3) Whether the person conducting the encryption research provides the copyright owner of the work to which the technological measure is applied with notice of the findings or results of the research; the time when such notice is provided. Where the provisions of the preceding two paragraphs are complied with, it is permissible to circumvent a technological protection measure prohibiting or restricting access to a	does not violate the Copyright Act or any other act or regulation. For the sole purpose of conducting encryption technology research, it is also permissible to develop or employ technological means for circumventing technological protection measures, or to provide such technological means to other persons conducting encryption research. 3. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(g) concerning exemption for encryption research.

Provisions	Comments
work. For the sole purpose of performing encryption research described in paragraph 1, it is permissible to develop and employ technological means to circumvent a technological protection measure prohibiting or restricting access to a work, and to provide such technological means to another person working collaboratively on the encryption research described in paragraph 1, or to another person working on encryption research described in paragraph 1 for the purpose of having that person verify the findings of the encryption research.	
12. "Reverse engineering" in subparagraph 8 of paragraph 3 of Article 80-2 of the Act means a person who has lawfully obtained the right to use a computer program identifying and analyzing elements of such computer program for purposes of achieving interoperability of an independently created computer program with other programs. Within the scope necessary to conduct reverse engineering described in the preceding paragraph, and where there is no infringement of copyright, it is permissible to circumvent a technological protection measure prohibiting or restricting access to a	1. Paragraph 2 of this point applies to circumstances in which it is permissible to circumvent access controls for purposes of conducting reverse engineering. 2. Paragraph 3 permits the development or employment of technological means to circumvent access controls and exploitation controls as necessary for identification and analysis to achieve the interoperability described in paragraph 1. 3. Example: For purposes of developing a computer program that is interoperable with a computer program of another firm, e.g.: a firm that is developing a program for

Provisions	Comments
computer program. As necessary for identification and analysis to achieve the interoperability described in paragraph 1, and where it does not constitute copyright infringement, it is permissible to develop or employ technological means to circumvent technological protection measures prohibiting or restricting access to or exploitation of a computer program. A person acting in compliance with the preceding two paragraphs may provide to others information acquired through reverse engineering referred to in paragraph 2 or the technological means adopted under paragraph 3, where provided solely for the purpose of achieving interoperability referred to in paragraph 1, to the extent that there is no violation of the Act or any other act or regulation. For purposes of this point, the term "interoperability" means the ability of computer programs to exchange information, and to use the information so exchanged.	that is developing a program for which interoperability with WORD or PDF programming [is sought] can utilize reverse engineering to develop an interoperable program. To conduct reverse engineering, after circumventing a technological protection measure attached to WORD or PDF programming, it can decode the other person's program to ascertain the structure and technology of the other person's program, but solely for purposes of developing an interoperable program. 4. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(f) concerning exemption for reverse engineering.

Provisions	Comments
13. "Other circumstances specified by the competent authority" in subparagraph 9 of paragraph 3 of Article 80-2 of the Act includes the following circumstances: (1) Lists of network locations blocked by commercial filtering software applications that are intended to prevent access to domains or websites, but not including lists of network locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network, or exclusively to prevent receipt of email; (2) Computer programs protected by dongles that prevent access due to malfunction, damage, or obsolescence; (3) Computer programs or digital content in formats that have become obsolete and which require the original media or hardware as a condition of access; (4) Literary works distributed in ebook format when all existing editions of the work, including digital text editions adopted by authorized entities, contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent	1. This point applies to circumstances specified by the competent authority in which it is permissible to circumvent access controls. 2. Examples: (1) Where the webmaster of a certain non-pornographic website, for purposes of ascertaining whether that website is being improperly blocked by a commercial filtering program, circumvents an access control used by that filtering program. (2) Where a program that a user has acquired lawful authorization to use is protected by dongles preventing use due to malfunction, and the user, for purposes of continuing to use the program, circumvents an access control used by that program. (3) Where it is an act of circumventing an access control used by a computer program that is in a program format that has fallen out of general use and become obsolete, when it subsequently becomes necessary to use the program format as a condition of access to the computer program. (4) Where it is an act of circumventing a technological protection measure used by an edition of an ebook that prevents the enabling of the ebook's read-aloud function and [prevents] the enabling of a screen reader to render the text in a specialized format, rendering blind readers unable to read the work, where done for purposes of enabling them to do so.

Provisions	Comments
the enabling of screen readers to render the text into a specialized format, rendering blind or readers with disabilities unable to read the work, for purposes of enabling them to do so. Under any of the circumstances in the subparagraphs of the preceding paragraph, it is permissible to circumvent technological protection measures prohibiting or restricting access to a work.	3. This point is adopted with reference to the US Digital Millennium Copyright Act Section 1201(a) concerning exemptions for circumvention of commercial filtering software, computer program hardware, computer program formats, and ebooks.
14. These Directions shall be reviewed at least once every three years.	The paragraph 4 of Article 80-2 of the Act charges the competent authority with periodically reviewing the Directions, so the period for such review is specified here.