

When Information Security Meets Intellectual Property in France and in the United States: Requirements Applicable to Certain DRMs

LAURENT SZUSKIN, JOANNA SZCZYGIEL, KEVIN C. BOYLE, AND ANDREW TING

The authors explore the ramifications of a French privacy law on industries as diverse as information technology suppliers to entertainment companies.

On August 1, 2006, the French Parliament passed law n° 2006-961 on copyright and related rights in the information society (the Law),¹ which implements the European Copyright Directive.² The adoption of the Law gave rise to substantial controversy during the parliamentary debates. In particular, the provisions in relation to the exception for private copying, interoperability, or the legal protection of the technical measures have been widely debated. The ramifications of the Law were so significant that they even drew the attention of commentators outside of France, and notably of U.S. writers.³

However, Article 15 of the Law went largely unnoticed, despite the

Laurent Szuskin is a partner in the Paris office of Latham & Watkins LLP. Joanna Szczygiel is an associate in the firm's Paris office. Kevin C. Boyle is a partner in the firm's offices in Washington, D.C., and Northern Virginia. Andrew Ting is an associate in the firm's office in Washington, D.C. The authors can be reached at laurent.szuskin@lw.com, joanna.szczygiel@lw.com, kevin.boyle@lw.com, and andrew.ting@lw.com, respectively.

fact that its impact on industries from information technology suppliers to entertainment companies is likely to be significant.

ARTICLE 15: A SUBSTANTIAL NEW OBLIGATION

Article 15 of the Law provides that:

- [• *The importation, the transfer from a member State of the European Community, the supply or the publishing of software likely to process protected works and which include technical measures enabling to remotely control directly or indirectly one or several functionalities or to access to personal data are subject to prior declaration with the State administration in charge of the security of IT systems. The provider, the publisher, or the person effecting the importation or the transfer from a member State of the European Community must provide to this State administration the specifications and the source code relating to the software in question, the source code of the libraries used if available, as well as all the tools and methods allowing to obtain such software from the provided source codes. The State administration in charge of the security of IT systems may request, if such software is based upon libraries and software elements created, imported or conceived by a third party, said third party to provide the above-mentioned elements. A decree issued by the State Council provides the conditions under which the declarations are filed and the above-mentioned technical information is to be provided.*
- *Software referred to in the first paragraph may be used in connection with automated data processing systems necessary for the protection of rights in protected works, only if it is operated in compliance with provisions of the Data Protection Act n° 78-17 dated January 6, 1978, and only if it is not used in a way that would violate secrecy protected by statute or public policy.*
- *The State is entitled to determine the conditions under which the software mentioned in the first paragraph may be used within automated*

data processing systems of State administrations, territorial collectivities, public or private operators in charge of installations of vital importance within the meaning of articles L. 1332-1 to L. 1332-7 of the Defense Code.

- *A decree by the State Council shall detail the conditions of application of the present article as well the nature of the automated data processing systems to which they apply.]*

Article 15 requires that any software including technical measures enabling remote control of functions or access to personal data must be declared and disclosed with its source code to the French state.

THE RATIONALE BEHIND ARTICLE 15

Article 15 was introduced in the *Assemblée Nationale*, pursuant to an amendment n° 273, which raised little parliamentary debate.

The alleged purpose of amendment n° 273 was to create a balance between the need for efficient copyright management systems (commonly named “digital rights management” or “DRM”) and the risks that such DRM systems compromise the security of computer systems of natural persons, companies, and government administrators by allowing the remote control of computer systems’ functions and remote access to personal data.

By requiring a declaration procedure for DRM software, Article 15 allows identification of the functions of a computer system that may be remotely controlled in order to prevent illegal uses such as data theft or destruction, spying, provoking a system failure, etc.

Article 15 appears to have been introduced in the Law as a result of the Sony BMG “rootkit” scandal in the United States. In 2005, Sony BMG distributed millions of audio CDs which contained DRM software that automatically installed itself into the user’s Microsoft Windows system without the user’s knowledge or consent. This DRM software limited the actions the user could take with regards to the audio CDs. Similar to a malicious “rootkit,” this DRM software concealed itself from the user and monitored the user’s activities on a continuous basis. Efforts to

delete the DRM software manually could render the user's CD drive inoperable.

In November 2005, Sony's DRM software became public knowledge. Sony recalled all unsold CDs containing the DRM software and offered an exchange for CDs without the DRM software. Sony also provided an uninstallation tool for the DRM software. However, the U.S. Computer Emergency Response Team of the U.S. Department of Homeland Security issued an advisory that both Sony's DRM software and its uninstallation tool could pose a security threat and introduced vulnerabilities to a user's system which could be exploited by other attackers.⁴

The furor over Sony's DRM software resulted in legal actions against Sony by the U.S. Federal Trade Commission ("FTC"), U.S. state attorney generals, and private class action litigants. To settle these legal actions, Sony agreed to pay millions of dollars to the various government agencies, pay certain amounts to each users who could prove that Sony's DRM software resulted in damage to their computers, and comply with certain disclosure and marketing obligations.⁵ In announcing the FTC's settlement with Sony, FTC Chairwoman Deborah Majoras stated: "Installations of secret software that create security risks are intrusive and unlawful. Consumers' computers belong to them, and companies must adequately disclose unexpected limitations on the customary use of their products so consumers can make informed decisions regarding whether to purchase and install that content."⁶

The Sony DRM software scandal resulted in heightened scrutiny of DRM software in the United States and in Europe.⁷ This heightened scrutiny is one of the rationales for the substantial new obligations for DRM software imposed by the French State through Article 15.

For a summary of the obligations, formalities, related authorities, and players, please see the chart at the end of the article.

THE MAIN OBLIGATIONS RESULTING FROM ARTICLE 15

The chart presents the obligations imposed by Article 15 and the entities responsible for compliance.

In any event, until the two decrees from the State Council have been issued and published, the interpretation and enforcement of Article 15 will remain unsettled.

COMPARATIVE APPROACH WITH THE SITUATION IN THE UNITED STATES: THE U.S. PERSPECTIVE

In the United States, there is currently no analogous law to Article 15 and no governmental authority specifically empowered to collect the source code of DRM software. As demonstrated by the Sony DRM software scandal, liability for supplying and publishing DRM software in the United States primarily arises from federal and state consumer protection laws enforced by the FTC and the state attorney generals. Such liability can be mitigated if the provider of the DRM software clearly discloses to consumers the existence and functionalities of the DRM software and requires consumers to give their fully informed consent prior to the installation and use of the DRM software. The Sony DRM software scandal demonstrates that governmental authorities and private class action litigants can and will take legal action against the providers of DRM software if these disclosure and consent requirements are not fulfilled.

Digital rights management is a fiercely contested issue in the United States, France, and other jurisdictions with significant economic and legal implications. Laws and best practices are rapidly evolving in this area in response to pressures from governments, industry, and consumers.

NOTES

¹ Published in the *French Official Journal* dated August 3, 2006.

² Directive n° 2001/29 dated May 22, 2001 on the harmonization of certain aspects of copyrights and related rights in the information of society. For more information about the Directive, see our related *Client Alert 540, The New Law on Copyright and Related Rights in the Information Society*, dated September 15, 2006.

³ *The International Herald Tribune, Confessions of criminals of the digital age*, Thomas Crampton, October 9, 2006.

⁴ United States Computer Emergency Response Team, First 4 Internet XCP

DRM Vulnerabilities, available at <http://www.us-cert.gov/current/archive/2005/11/17/archive.html#xcpdrm>, November 17, 2005.

⁵ See, e.g., “*Court Approves Sony BMG Settlement*,” available at http://www.consumeraffairs.com/news04/2006/05/sony_bmg_settlement.html, May 23, 2006; “*Sony BMG Settles Root-Kit Suits for \$4.25 Million*,” available at http://www.consumeraffairs.com/news04/2007/01/sony_bmg_states.html, January 2, 2006; “*Sony BMG Settles California Case*,” available at http://www.consumeraffairs.com/news04/2006/12/ca_bmg.html, December 19, 2006; and “*Sony BMG Settles FTC Charges*,” available at <http://www.ftc.gov/opa/2007/01/sony.shtm>, January 30, 2007.

⁶ “*Sony BMG Settles FTC Charges*,” available at <http://www.ftc.gov/opa/2007/01/sony.shtm>, January 30, 2007.

⁷ See, e.g., “*Legal proceedings in Italy by ALCEI for a ‘criminal’ offense*,” available at <http://www.alcei.org/?p=22>, November 5, 2005.

⁸ *JurisClasseur on Competition and Consumer law*, chapter 1010, n° 92, *Lamyline on Consumer law*, n° 7068, *Dalloz* 1998, p. 37, note by Alain Lacabarats.

⁹ Such obligation already existed under law n° 78-17 of January 6, 1978 on computerized data, files and civil liberties as modified by law n° 2004-182 of August 6, 2004.

¹⁰ Such definition is provided by Article 3 of the Data Protection Act.

Obligations Set Forth Under Article 15	Entities Responsible for Compliance	Applicable Sanctions
<p data-bbox="265 465 520 596"><i>Obligations toward the state administration in charge of the security of IT systems</i></p> <ul data-bbox="265 634 520 1346" style="list-style-type: none"> <li data-bbox="265 634 520 990">• Prior declaration to the French State administration of any software that includes technical measures enabling to control remotely one or several functionalities directly or indirectly or to access to personal data; <li data-bbox="265 996 520 1346">• Disclosure of the corresponding source codes and specifications, and of all the tools and methods allowing to obtain such software from the provided source codes. The information to be communicated is thus particularly broad. <p data-bbox="265 1384 520 1543">Two decrees issued by the State Council will detail (i) the conditions under which prior declarations are filed, and</p>	<ul data-bbox="555 634 801 1427" style="list-style-type: none"> <li data-bbox="555 634 801 877">• The software importer, i.e., the person who purchases abroad such software in his/her own name and on his/her behalf in order to sell such goods in France.⁸ <li data-bbox="555 883 801 1296">• The person effecting the transfer from a member State of the European Community, it being specified that in such case the required declaration and disclosure of source code could probably not be made without the assistance of the software supplier/manufacturer. <li data-bbox="555 1301 801 1358">• The software supplier. <li data-bbox="555 1363 801 1427">• The software publisher. 	<ul data-bbox="836 634 1082 821" style="list-style-type: none"> <li data-bbox="836 634 1082 821">• Absence of specific sanctions set forth by the Law. (The decrees will probably specify the applicable sanctions.)

Obligations Set Forth Under Article 15, cont.	Entities Responsible for Compliance, cont.	Applicable Sanctions, cont.
<p>(ii) the conditions of application of Article 15. Such decrees have not yet been published.</p> <p><i>Obligations toward the French data protection authority (“CNIL”)</i></p> <ul style="list-style-type: none"> • Software covered by Article 15 may be used in connection with automated data processing systems only if made “<i>in compliance with provisions of the Data Protection Act n° 78-17 dated January 6, 1978</i>”: compliance with the Data Protection Act requires, <i>inter alia</i>, prior formalities (declaration or request for authorization as the case may be) to be filed with the CNIL.⁹ 	<ul style="list-style-type: none"> • The data controller, i.e., a person, public authority, department or any other organization who determines the purposes and means of the data processing.¹⁰ 	<ul style="list-style-type: none"> • Criminal and administrative sanctions are set forth by the Data Protection Act and can go up to five years’ imprisonment and a fine of €300,000.