# ADDITIONAL DEVELOPMENTS—FOREIGN AND INTERNATIONAL LAW

## *EUROPEAN PARLIAMENT PASSES TELECOMMUNICATIONS DIRECTIVE*

On May 29, 2002, the European Parliament approved a Communications Data Protection Directive ("directive") allowing countries to force telecommunication companies to keep detailed records of customers' data for an unspecified period. The European parliament passed the controversial update to the 1997 directive on privacy in the telecommunications sector by a vote of 351-133. The directive grants police access to transmission data for e-mail, phone calls, internet use, faxes, and pager messages to deter terrorist attacks. The European Union's fifteen member states are required to grant their approval before the directive goes into effect.

If approved, the legislation would require the European Union's 15 member countries to draft laws requiring ISPs and telephone companies to keep track of phone calls, Internet surfing, e-mails, faxes and even pager messages, for an unlimited time period in case the data is needed by law enforcement authorities. Generally, European law takes precedence in cases where a directive conflicts with national laws. Thus, approval by the member states is expected, meaning that the directive may go into effect as soon as a few months, but almost certainly within five years.

Forty different civil liberties groups in Europe and the United States and an online petition have gathered over 16,000 signatures opposing the directive. These opponents urged parliament members to vote against the data-retention measure. Although the measure passed, the last minute addition of text requiring that data retention constitute a "necessary, appropriate and proportionate measure within a democratic society to safeguard national security," and that it must be done in accordance with the tenants of the European Convention on Human Rights and Fundamental Freedoms, weakened the directive's power.

An aggressive campaign will be waged by civil liberties groups who continue to denounce the measure as entitling governments to blanket general surveillance of the whole population. They say the measure would enable police to spy on citizens. Although police will still require a warrant to intercept the content of electronic communications, the new legislation means they will be able to build up a complete picture of an individual's personal communications, including who they have emailed or phoned and when, and which Internet sites they have visited. From mobile phone records, police will also be able to map people's movements because the phones communicate with the nearest base station every few seconds. In urban areas, the information is accurate to within a few hundred meters. The next generation of mobiles might be employed to pinpoint users' locations to within a few meters. Currently, telephone records are kept only for a couple of months for billing purposes before being destroyed. The communications industry opposes data retention, questioning the feasibility and cost of storing such vast amounts of information.

## *EUROPEAN COUNCIL DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATION*

On July 12, 2002, the European Parliament adopted an updated Communications Data Protection Directive. This Directive, 2002/58/EC, toughens requirements regulating unsolicited advertising using personal data for marketing purposes. The new directive attempts to take account of technological changes and make the provisions as technology-neutral as possible. Member States have fifteen months to incorporate these provisions into their national legislation and bring their regulations into compliance with the new directive.

The new directive has serious implications for both the use of cookies and the sending of direct marketing e-mails. The directive allows the use of cookies provided that two requirements are met: first, the website user is given 'clear and comprehensive' information about the function of the cookie, and second, the website user is offered the right to refuse the cookie. The directive requires direct marketers to obtain prior explicit consent of the website user before e-mails, faxes, or automatic calling machines are used. Additionally, all direct marketing e-mails must provide a valid address for 'unsubscribe' requests. The only exception to the more stringent regulation of direct marketing e-mails is when a company markets products or services similar to a previous transaction that occurred between the individual website user and the company.

The new directive includes several important changes over predecessor data protection directives, 95/46/EC and 97/66/EC. First, it contains new definitions for electronic communications and services aiming to ensure technological neutrality and clarify the position of e-mail and the use of the Internet. Second, it enables value added services based on location and traffic data where subscribers consent, such as location based advertising to mobile phone users. Third, it prohibits charging subscribers for exercising the right not to appear in public directories. Fourth, new information and consent requirements on entries in publicly available directories, including a requirement that subscribers are informed of all the usage possibilities of publicly available directories, are introduced. Fifth, it extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail, UCE or Spam, and SMS to mobile telephones. Sixth, the directive clarifies that Member States are not prevented from introducing provisions on the retention of traffic and location data for law enforcement purposes. Seventh, and last, the directive introduces controls on the use of cookies on websites.

Both the Council of Ministers and the European Union recognize that development of a frontier free market increases the cross-frontier flows of personal data among Member States of the European Union. The directive recognizes that, as data subjects, individuals are entitled to information explaining the processing of personal data. Further, individuals must not only have access to that data, but also receive an explanation as to how any significant decisions affecting them are made.

This directive is part of a package of five directives agreed upon between the Council of Ministers and the European Parliament establishing a framework for the regulation of electronic communications networks, services and associated facilities throughout the European Union.[1] By harmonizing data legislation, the European Union

1. (1) Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive - FD); (2) Directive 2002/20/EC on the authorization of electronic communications networks and services

expects to achieve free movement of information, including personal data. At the same time, the European Union hopes to ensure the protection of any person concerned. These directives collectively attempt to remove potential obstacles to such flows and to ensure a high level of protection within the European Union.

(Authorization Directive - AD); (3) Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - USD); (4) Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and services (Access and Interconnection Directive - AID); and (5) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

## *KABUSHIKI KAISHA SONY COMPUTER ENTERTAINMENT V. STEVENS*

*[2002] 55 I.P.R. 497 (Fed. Ct. Austl.)*

The Federal Court of Australia ruled on whether the disablement of a computer game console's technological device that ensures the use of licensed software violated Australian copyright law. The Federal Court addressed whether the device represented a "technological protection measure" under Sections 10(1) and 116(A) of the Copyright Act and specifically ruled on whether the portion of the game software program stored in the console's RAM satisfied the material form requirement for a protected reproduction of a copyrighted work.

The Sony companies are owners and/or exclusive licensees of more than 150 copyrighted games for the Sony PlayStation game console. Sony builds a hidden track containing an encrypted access code into each CD-ROM game created for use on the PlayStation game console. The PlayStation game console contains a device that prevents the play of any CD-ROM game not containing the encrypted code. By doing so, the device not only generally discourages the making of illegal copies of the CD-ROM games, but it also specifically prevents the temporary storage of a portion of the CD-ROM software into the game console's RAM. Defendant Eddy Stevens modified Sony PlayStation game consoles to disable the device and allow the play of games not containing the encrypted code.

The Federal Court held that the modification did not violate Australian copyright law. The court held that Sony did not create a "technological protection measure" as defined under Section 10(1) of the Act, thereby precluding Sony's device from protection under Section 116A. First, the court found that the device's practical effect of discouraging copyright violations, which predated attempts to gain access to or copy the works, did not alone make the device a "technological protection measure." The court reasoned that the device must be designed to function, by its own processes and mechanisms, to prevent or hinder an act of copyright infringement, not simply discourage it. Second, the device also failed as a "technological protection measure" because the temporary storage of a portion of the software program from the CD-ROM to the PlayStation game console's RAM was insufficient to constitute a reproduction of a substantial part of the computer program "in a material form." While other cases had found programs copied to personal computer RAM to be in material form, the court distinguished the copying to PlayStation RAM on the grounds that the data temporarily stored in the PlayStation RAM cannot be used to reproduce a substantial part of the copyrighted work. The court found insufficient evidence existed to determine whether or not a reproduction in material form occurred when the data stored in the PlayStation RAM was transferred to the GPU.

## *GALERIE D'ART DU PETIT CHAMPLAIN, INC. V. THEBERGE*

*[2002] 210 D.L.R.4th 385 (Can.)*

The Supreme Court of Canada addressed whether, in lifting the ink images of an artist's work off of authorized paper posters and transferring the images to a canvas substrate, several art galleries and a publishing firm had infringed the artist's copyright.

Claude Theberge, a painter of some international renown, contracted with a publishing firm to reproduce his works on paper posters and other stationary products. Appellant art galleries legally purchased those works and then used a chemical process to lift the ink off of the original paper product and reapply the image to canvas backing, creating a more painterly result. Theberge alleged that the process violated his copyright on the paintings and applied to the Quebec Superior Court for injunction, damages, and most significantly, obtained a writ of seizure before judgment. However, the Superior Court eventually rejected his copyright infringement claim and quashed the seizure. The Court of Appeal disagreed, found infringement, and allowed seizure of the goods. The art galleries appealed to the Supreme Court.

The Supreme Court held that the transfer of original lawfully purchased poster images to canvas did not constitute copyright infringement because no new reproductions were created in the process. In effect, the Court believed that copyright infringement could not be maintained absent actual "copying" and here there was no net increase in the number of total physical images. As a result, the Court allowed the appeal and ordered the seized goods returned. The Court reasoned that an opposite finding would lead to excessive control of copyrighted works subsequent to sale and would severely limit utilization by the eventual purchaser.

The Court believed that Theberge's claim could be more properly characterized as a claim of infringing his moral rights, which is addressed by a different section of the Copyright Act and requires that the modification cause "prejudice of the honor or reputation of the author." The Court reasoned that because of the drastic consequence of the seizure, the Parliament would require prior judicial review before any seizures take place based on an assertion of violation of moral rights. Therefore, the Court concluded that Theberge's seizure before judgment was not warranted.

## *SOCIETY OF COMPOSERS, AUTHORS & MUSIC PUBLISHERS OF CANADA V. CANADIAN ASSOCIATION OF INTERNET PROVIDERS*

*[2002] 4 F.C. 3 (Fed. Ct.)*

The Society of Composers, Authors and Music Publishers of Canada (SOCAN) applied to the Canadian Federal Court of Appeal for judicial review of the decision reached by the Copyright Board that exempts Internet intermediaries from paying royalties for music transmitted over the Internet.

The judicial review raised three issues: (1) whether service providers and host servers merely provide the means for communication and are therefore immune from paying royalties on content transmitted; (2) whether materials transmitted from foreign servers are exempt from Canadian royalties as the Board had determined; (3) whether Internet intermediaries authorize the communication of music on the Internet by providing access to and storage of the content and are thus liable to pay royalties.

As to the first question, the court largely agreed with the Board that the normal activities of the Internet intermediaries satisfied the three requirements to be classified as telecommunications set forth in paragraph 2.4(l)(b) of the Copyright Act. Namely: (1) the activities are to provide "means" of telecommunication; (2) the activities are necessary for the communication and (3) the activities are the only activities of the Internet intermediaries. Therefore, Internet intermediaries are exempt form paying royalties to copyright owners. However, the majority disagreed with the Board in finding that caching is not necessary for the communication to occur, and therefore concluded that cashing is not protected by paragraph 2.4(l)(b).

As to the second question, the court rejected the Board's decision and held that transmissions originating from servers outside of Canada may still face Canadian royalties, since infringement only occurs at the request of the end user. The court found that the narrow jurisdictional determination by the Board severely limited the ability of copyright holders to protect their works in the Canadian market, and concluded that a test of "real and substantial connection with Canada" should be applied to determine whether a royalty may be made payable in Canada. The court proposed that the location of the content provider, the end user, and the host server should all be important factors in the test.

As to the third question, the court found it reasonable for the Board to conclude that Internet intermediaries do not "authorize" the communication of material requested by end users from host servers by providing their core services and equipment, since normal activities of the operators of host servers only provide passive means for others to communicate. As such, the service provider is not in a position to authorize content, and thus incur liability. The court likened the role of host servers to that of passive facilitators, rather than viewing them as actively sanctioning infringing material.