CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 157 years

FRIDAY, OCTOBER 26, 2012

Chicago Daily Law Bulletin

Volume 158, No. 211

EU privacy laws hinder copyright enforcement for U.S. owners

The ongoing battle against digital piracy has a new stumbling block in the form of European Union privacy laws. While U.S. website operators routinely gather data about end users, and sell it, in the EU such commercialization of private data has been largely prohibited since 1998. Unfortunately for copyright owners, privacy rights in the EU have also moved further away from U.S. policy to the point where they now challenge the ability of U.S. owners to prevent digital piracy from sites originating in the EU, including most of Europe. Wiggle room still exists, but enforcement methods must be reconfigured to survive this latest challenge.

A copyright owner's toolbox for combating online piracy has shrunk considerably over the past several years. Much touted solutions such as the "three strikes rule" (prohibiting access after three instances of copyright infringement) and the Anti-Counterfeiting Trade Agreement (ACTA) have largely proved ineffective in the face of growing opposition to any effort to reduce Internet access.

As social media, digital communications and e-commerce play an increasingly dominant role in end users' lives, the legal desirability of prohibiting Internet access to prevent copyright infringement becomes more tenuous. Early public challenges focused on the adverse impact of such prohibitions on "access to information" and "free speech" concerns. Present challenges, particularly in the EU, have raised the bar to include privacy protection. As access to personal information becomes technologically easier, legal strictures on such access have risen markedly.

The EU Database Privacy Directive requires the protection of "the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to processing of personal data." (Article 1). Created in the early era of the Internet, before it morphed into a vibrant outlet for social media and piracy, this protection of personal processing data was given new life in November 2011 in *Scarlet Extended v. SABAM.* (Case C-70/10). SABAM, a Belgian collective rights organization, had obtained an injunction obligating Scarlet, a social networking site, to install a filtering system that would allow Scarlet to monitor and block end users' unauthorized file trading of SABAM's members works. In overturning the injunction, the European Court of Justice (ECJ), the equivalent of the Supreme Court for the EU, acknowledged that such a filtering system "pursues the aim of ensuring the protection of copyright." It further recognized that the protection of intellectual property rights is enshrined in the Charter of Fundamental Rights of the European Union, which specifically provides "intellectual property shall be protected." (Article 17(2)).

This right, however, is not "inviolable." Instead, the ECJ held that it must be proportionally balanced against "other fundamental rights." In this case, the court held that the balance leaned too far in favor of intellectual property protection and failed to respect "the right to protection of personal data."

This past February, in *SABAM v. Netlog, NV* (Case C-360/10), the EJC reaffirmed its refusal to approve preventive monitoring systems to protect copyright where such systems require the Internet service provider "to actively monitor almost all data relating to all of its service users in order to prevent any future infringement."

By addressing its comments to the particular injunction at issue, however, the ECJ left the door open for a more narrowly crafted monitoring system to survive a privacy challenge. Such survival may have occurred in *20th Century Fox Film v. BT (Newzbin2)* (Case No: HC10C04385), where the British High Court of Justice upheld an injunction requiring use of Cleanfeed technology to block unauthorized file trading in the plaintiff's copyrighted films. Cleanfeed is a filtering system that blocks end users' access to specified website addresses (URLs). Significantly, the court found the injunction met the required proportionality test because it specified the technology to be used and allowed for reconsideration of the scope of such monitoring should the circumstances change.

Unexpectedly, privacy concerns have proven less problematic in connection with end user identity disclosure. Similar to other enforcement cases, the ECJ has insisted on proportionality in balancing copyright and privacy interests. Surprisingly, the ECJ held in 2008 in *Promusicae v. Telefonica de España* (Case C-275/06) that identity disclosure was not required "to ensure effective protection [of copyright] in civil procedures." Yet despite the initial rejection of obligatory identity disclosure, the ECJ has generally found such disclosure demands under national laws meet the proportionality test.

Thus, in April 2012 in *Bonnier Audio AB v. Perfect Communication Sweden AB* (Case C-461-10), the court upheld Sweden's domestic disclosure laws that required "clear evidence" of an infringement, that the requested information "facilitates" the investigation and that "the reasons for the measure outweigh the nuisance or other harm" the disclosure may entail. Since the national legislation enabled the court to "weigh the conflicting interests involved ... taking due account of the requirements of the principle of proportionality," the ECJ held it was "likely, in principle to ensure a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by Internet subscribers or users."

Despite the strong protection that personal privacy rights receive under EU law, at least in connection with end user disclosure, copyright owners should be able to secure such disclosures provided they have strong evidence of potential infringement.

Reliance on computer bots and other technological measures for seeking unauthorized postings is not necessarily precluded but should be combined with filtering or some other method for assuring the validity of claims of potential infringement.

For the present, carefully crafted injunctive relief might also be available so long as such relief is narrowly circumscribed to avoid costly or extensive monitoring of end user activities. The one unpredictable factor is whether privacy rights in the EU will become even stronger. Given that a current draft EU privacy regulation goes so far as to grant end users a "right to be forgotten" through erasure of personal data (Article 17), copyright owners can only hope that the precarious proportionality balance that favors copyright protection currently does not tip too far in the opposite direction.

GLOBAL IP

DORIS ESTELLE LONG

Doris Estelle Long is a law professor and chairwoman of the intellectual property, information technology and privacy group at The John Marshall Law School. She has served as a consultant on IPR issues for diverse U.S. and foreign government agencies, including as attorney adviser in the Office of Legislative and International Affairs of the USPTO. She can be reached at 7long@jmls.edu.

> ***"As access to personal information becomes technologically easier, legal strictures on such access have risen markedly."***