From Censorship to Cartelisation?: ISPs and their management of undesirable content

Lilian Edwards
Professor of Internet Law, University of Southampton
Email: L.Edwards@soton.ac.uk

Abstract

ISPs, as the natural "gatekeepers" to the Internet, have the power to control what content (including text, images, music and video) is accessed by their subscribers. Since they are neither public sector bodies nor courts, their practice in exercising this power is largely invisible, with only their Acceptable Use Policies (AUPs) made public. Accordingly, efforts have been made repeatedly to determine how ISPs deal with "notice and take down" (NTD) requests1, and more generally, to see what role if any ISPs perceive themselves as playing: whether censors, moral guardians, protectors of freedom of expression, technical neutrals, or businesses simply concerned with profits. A further connected issue is that much illegal activity is likely to be perpetrated from subscribers to ISPS under cover of anonymity or pseudonymity. Issues thus also arise as to how ISPs asked to disclose the name of a subscriber choose to strike a balance between subscriber rights of privacy, and the state's (and victims') right to enforce laws.

From August 2005 to September 2006, Edwards, under the auspices of the Arts and Humanities Research Centre for Intellectual Property and Technology Law, carried out a multi-levelled study for the first time researching in one survey, ISPs and their handling of (a) illegal and actionable content and (b) disclosure of the identities of their subscribers. The study comprised (a) interviews with key industry and regulatory players (b) a detailed questionnaire sent to 48 organisations, with a 35% response , and (b) a follow-up online survey which sought to determine industry practice in relation to "notice and disconnection" of "bandwidth hogs".

The preliminary trends emerging are interesting. NTD has moved from being the remedy of the occasional disgruntled individual to an institutionalised and often automated process, particularly in the domains of copyright infringement and child pornography. Bodies such as the BPI and the Internet Watch Foundation (IWF) now have close working relationships with an ISP industry anxious to avoid "hard" legal regulation. Illegal content is increasingly hosted off-shore, thus shifting the remedy sought from NTD to content filtering and access-prevention. The government is interested in promoting the use by ISPs of "cleanfeed"-style upstream censorship, such as BT now supply, to prevent, eg, the spread of materials relating to terrorism. It may also need to seek the assistance of ISPs to fight network insecurity (eg scanning for "zombified" home user machines).

Questions need to be asked if this convergence of interests from the state, the law enforcement agencies (LEAs) and the copyright industries in "enrolling" the assistance of ISPs is leading us potentially towards "cartelised" invisible online censorship. Privacy rights may also be lost if the ISP industry decided to reduce risk by assisting private as well as LEA interests. There may be a move towards "notice and disconnection" rather than NTD. Finally, at present ISPs are protected by the immunities granted in 2000 by the EC E-Commerce Directive: it is suggested these will come under fire in the upcoming EC review.

[1] Oxford Study, Dutch study, ISPA survey.