 Illegal activities, preventative technologies & ISP immunity: Where should the buck stop?

Dr. Carlisle George
School of Computing Science, Middlesex University,
Email: c.george@mdx.ac.uk

Abstract

The Electronic Commerce Directive sets out rules regarding the liability of Internet Service Providers (ISPs) in the European Union. Under these rules, three categories of increasing liability exist, namely being a mere conduit, caching and hosting. As a mere conduit an ISP is not liable for damages or any criminal sanction as a result of a transmission (of content) where the ISP does not initiate the transmission, did not select the receiver of the transmission and did not select or modify the information contained in the transmission. Where an ISP is involved in caching, it is also not liable for damages or any criminal sanction resulting from the transmission of content, subject to compliance with certain rules such as not modifying the information (in the transmission), and complying with conditions on access to that information. ISPs that host content are not liable for damages or any criminal sanction as a result of the storage of illegal content unless they are aware of such content and fail to remove it. Finally the law does not impose a general obligation on ISPs to monitor any information transmitted or stored, neither is there a general obligation to actively seek out illegal activity.

In the 2007 case of Sabam vs Tiscali (Scarlet) a Belgian court (of first instance) ordered an ISP (Scarlet) to filter traffic (using Audible Magic software to scan peer-to-peer network traffic) to prevent file sharing of unauthorised copyright material. This ruling has sparked an interesting debate regarding the limits of the protection granted to ISPs under the E-Commerce Directive, and the rights of copyright holders under the EU Copyright Directive to take action against intermediaries whose services are used to pirate copyright material. The debate raises wider issues related to the extent of ISP liability in general, especially in the face of new technologies that can be used for filtering, identifying and blocking illegal content. Indeed, recently, ISPs have come under increasing pressure from politicians and legislators (in the UK, Australia and Italy among other countries) with regard to blocking illegal and offensive content. In some countries such as China, ISPs are obligated by law to monitor and control transmitted content. This paper examines
the current debate and the wider question of whether ISPs can or should be held liable for some kinds of illegal online activities, especially where technically feasible methods can be used to monitor and control these activities. The paper discusses the relevance and adequacy of the present law on ISP immunity, in the present climate of increasing illegal online activities and also discusses technologies that can be use by ISPs to police online activities. The paper further questions whether the present law needs to be amended in the face of new technological capabilities. Finally the paper gives recommendations for possible ways forward for the future.