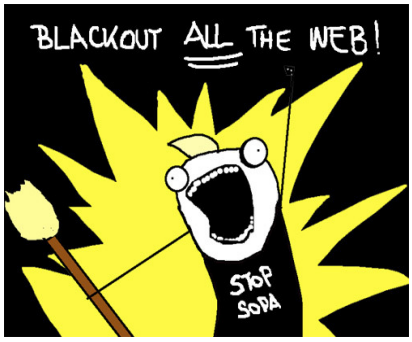
By Maxime Lambrecht, 26 January 2012

The web goes dark, Megaupload goes down (or why there was no need for SOPA/PIPA after all)

The day after the unprecedented tide of protest against the SOPA/PIPA bills, the American Department of Justice ran a vast international operation that led to the shutdown of Megaupload and the arrest of the managers of the 'digital locker' website in New-Zealand, on grounds of copyright infringement conspiracy. Some might see it as a peculiar coincidence that the positive momentum in favor of openness and Net neutrality was almost immediately slashed by the media coverage of a clear-cut piracy case, with the Anonymous playing the perfect role of the teenage rebels defending their preferred means of downloading the latest Lady Gaga. But in fact, the takedown of Megaupload might provide a rather good argument for the defenders of an open Internet : if such an indictment against a foreign company is already possible, then the SOPA/PIPA bills are unnecessary.



The Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA), were two bills introduced in the US Congress, aiming to fight « rogue websites », i.e. foreign sites dedicated to copyright infringement (for a comprehensive summary, see Masurlaw). Whereas the existing provisions in the DMCA (also provided by the european Infosoc directive) focused on the removal of infringing content by internet service providers (such as Youtube, Dailymotion, or … Megaupload), the SOPA bill further allowed the right holders to send notice requiring payment providers (such as Paypal, etc.) and advertising services (e.g. Google Adwords) to stop serving the site. As with the DMCA, these intermediaries would be immune from any liability for any damage due to actions taken against alleged infringers, which gives them incentives to comply zealously. Moreover, the bills enables the Attorney General to bring suit against « foreign infringing sites », and have a court order that the site be cut off by services providers, search engines, payment providers, advertising service, and (in PIPA) even DNS servers (that runs internet adresses, or URL). As the DNS blocking solution has already been critized here, I'd like to emphasize the issue of due process : whenever a right holder deems that a website violates its copyright, he could ask a court to order, without any prior opportunity for hearing for the defendant, that the entire website be shut down.

After a global web protest seeing more 7 million signatures and 115 000 websites going dark, the sponsors of the bills finally announced that they were shelved.

What is immediately apparent from the Megaupload case, regardless of its merits, is that a US court can *already* issue an indictment against a foreign website, and have its domain name blocked. The adress http://www.megaupload.com/ now points to a banner from the FBI and the Department of Justice, stating that « This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. district Court ». Note that the DNS blocking by a US court produces effects worldwide, whereas the same measure taken by a Belgian court in another case only affects national users. This is probably because the District Court of Virginia acted on the primary domain name servers of the network, whereas the court of Antwerpen order applied only to belgian Internet providers Telenet and Belgacom. This might trigger some concern about the continuing dominance of the United States on the Domain Name System of the Internet, and its control on all the widespread .com and .org domains.

The main conclusion is that under the current legal regime, there seem to be sufficient « enforcement tools » at hand. The objection (made by RIAA's spokewoman Cara Duckworth) about the difficulty of enforcing the law in countries such as Russia or China, unlikely to cooperate with a US or European investigation, does not seem to build enough ground to support new legislation. First, these repressive regimes might not be so hospitable towards website hosting unrestricted content, for political reasons. Second, decent download speed (the principal advantage of file lockers compared to peer-to-peer file sharing) requires to set up servers located near the users, which would therefore make them reachable within a non-lax IP jurisdiction.

Certainly, court procedures take time, but it is the cost of justice : some amount of efficiency in law enforcement must be traded off against due process. There's a tendency in copyright law to assume that the best way to speed up court process are to skip the procedural guarantees of a fair trial, or to skip the trial altogether. Indeed, in addition to the legal means against piracy, the actors are more and more resorting to para-legal enforcement. We are actually seeing a growing tendency that has been labelled the « invisible handshake » (Birnhack & Elkin-Koren), where a convergence of interest between the state and private parties often leads the power

ful intermediaries of the digital environment to cooperate to law enforcement and control of the network, among themselves or with the government. This can be seen in such trivial mechanisms as the « notice and take-down » systems, or more elaborated private initiatives such as the « six strikes » agreement against copyright (the private version of the french Hadopi law – see also James Grimmelmann). Whereas the efficiency

of enforcement is certainly increased, this is not always for the best. Not only does some legal provisions incentivize intermediaries to adopt an overreaching view of copyright enforcement, to the detriment of users claims of 'fair use' (with the previsible chilling effects on speech), but often private companies already have well enough (if not too much) incentives to accede to takedown requests made by powerful actors, whatever their legitimacy. Great powers coming with great responsibilities, the control that the intermediaries have on information must not remain unchecked. A good illustration of this worrying trend is the speed with wich payment providers, hosting services, and domain name services responded to suggestions by US officials that « No responsible company – whether American or foreign – should assist WikiLeaks in its efforts to disseminate these stolen materials » (Senator Joe Liberman, quoted by Yochai Benkler in yet another excellent paper), eventhough Wikileaks was not carrying out any illegal activity, and could have quite arguably been entitled to constitutionnal protection under the freedom of the press.

Even if the Protect IP / Stop Online Piracy Act bills are probably halted for the time being, their provisions still echoed a growing trend towards a hurried delegation of copyright enforcement to private actors that have their own agenda and often couldn't care less about balancing copyright protection and users' privileges, or protecting freedom of speech and the open Internet. This is a perversion of the promises of the early Internet utopies : where the network was supposed to emancipate the individuals from the channeling of information by mass media and economic interests, the current evolution of the Internet regulation could actually lead to a far worse state of affairs. It is this trend that should spark our worries, more than the short-term legal problems possibly caused by digital lockers like Megaupload.

Maxime Lambrecht