

By Alain Strowel, 3 February 2012

Megaupload, WikiLeaks: when online payment intermediaries seem to apply different standards



As everyone knows, communicating on the Internet has nothing to do with a direct, face-to-face conversation. (The Internet, however, wrongly gives the impression that those who write and speak to one another are not relying on intermediaries). There are many layers of technical infrastructure that permit the link between two Internet users.

The regulation of Internet therefore must cover those intermediaries. The safe harbour notice and takedown procedures adopted in various countries, for example in Europe by the 2000/31 e-Commerce Directive, represented the standard for assessing what can be required from technical intermediaries in order to regulate the online exchange of information (By the way, the e-Commerce Directive is really a model for intermediary liability as it is not limited to copyright violations, but covers infringements to privacy, reputation, etc. contrary to the much narrower U.S. Digital Millennium Copyright Act.) Under this model, as summarized by Y. Benkler (see [here](#)), “providers of caching, web-hosting, and search engines and web directories were required to have a procedure in place for receiving notices regarding specific offending materials, and for taking down those materials; but they were not required to search out such content themselves or to block entire sites”. Whether this was enough or not to have a balanced government of what technical intermediaries should undertake remains to be demonstrated. There are signs that more — but not much more — should be required from some intermediaries who refuse to cooperate when their revenues can be negatively affected, but do not hesitate to zealously follow official instructions when this has no major impact on their sources of revenues.

Since the 2011 WikiLeaks saga and the more recent Megaupload cases, attention has shifted towards other intermediaries, in particular towards online payment systems. Money is the sinews of war — it is the blood of online conversations and dealings too. The U.S. indictment of the “Megaupload Conspiracy”, comprising the now famous Kim Dotcom, its acolytes and several companies who together were running several websites (Megaupload.com, Megavision.com, etc.), describes the group as “a worldwide criminal organization whose members engaged in criminal copyright infringement and money laundering on a massive scale” — where large money laundering is involved, it is difficult to ignore the role of payment intermediaries. In the case of Megaupload.com, income came primarily from two sources: premium subscriptions and online advertising, which respectively generated \$150 million and \$25 million (I follow here the description made in the instructive 72 page long indictment). Premium subscriptions have been available for online purchase for a few dollars per day or for around \$260 for a lifetime. In exchange for the payment, the cyberlocker site offered a fast distribution of copyrighted works. The revenues from the online advertising on the Mega sites were important thank to the popularity of the infringing materials. In addition, the Conspiracy had an “Uploader Rewards” Program which promised premium subscribers transfers of money and other financial incentives to upload popular works to the Mega computer servers. This could only be managed on a global scale thanks to the services of PayPal, a U.S.-based global e-commerce business involved in approximately 15% of global online payments. The indictment further states that the Megaupload Conspiracy’s PayPal account had been used to receive the premium subscriptions and to pay the U.S. (Carpathia Hosting) and Dutch (Leaseweb) companies operating the servers. Over the last 5 years, the PayPal account of the Mega Conspiracy “has received in excess of \$110,000,000 from subscribers and other persons associated with the Mega Conspiracy” (p. 19 of the indictment). It was probably difficult for PayPal to completely ignore the situation... Apparently, PayPal was not really ‘proactive’ in this case (at least, the company was much more prompt to express its concerns against the PIPA and SOPA bills than to tackle the Megaupload issue!).

This conduct is worth to compare with the way PayPal acted in the WikiLeaks case — although the law did not prohibit the publication of the leaked documents in this case. As summarized by Y. Benkler, the constitutional privilege allowed WikiLeaks to publish the documents; nevertheless, several American political figures denounced the disclosure. A letter of the State Department to WikiLeaks did not claim that WikiLeaks had infringed the law, but vaguely asserted that the law had been broken (by someone). This insinuation was enough to have PayPal discontinuing its service to WikiLeaks. This denial-of-payment decision (followed by the similar moves of Visa, MasterCard, etc.) immediately put WikiLeaks under a strong pressure as its operations depended on the continuing small donations by Internet users (nothing compared to the \$110,000,000 transiting on Megaupload’s PayPal account). It is strange to see that a simple insinuation of illegality has created a fast denial-of-payment in one case — a denial that affected an Internet tool for democratic transparency -, while quite a clear breach of the law, including on money laundering, has apparently not resulted in any responsible reaction in another case...

By the way, I do not agree that the recent legal developments in Megaupload show that no improvement of the legal framework is needed to fight online piracy. The indictment of Kim Dotcom and his co-accused was probably made possible because they were in New Zealand and because Megaupload had servers in Virginia, U.S. and the Netherlands (see also the 28/1/2012 FT article: [US in mega battle to bring in Mr Dotcom](#)). Would the case involve countries where

copyright piracy is blended with a mafia-type of culture, or reinforced by an anarchic situation or a form of State authoritarianism, the outcome would probably have been very different (on this, I respectfully disagree with M. Lambrecht's view presented in his otherwise very interesting and well-informed article published on ipdigit [here](#)). This is why new rules at international level such as those of the Anti-Counterfeiting Trade Agreement (ACTA) are probably needed so as to ensure a level-playing field in the countries where the rule of law, and its inherent safeguards, need to be reinforced.

PayPal itself is well aware of the changing legal environment. In its recent filing before the U.S. Securities Exchange Commission (SEC), eBay (the parent company of PayPal) states that the legal climate is "becoming more adverse" (probably eBay has in mind the recent decision of the Court of Justice of the EU in the [L'Oréal v. eBay](#) case about secondary liability for trademark infringement):

"We are continuously seeking to improve and modify our efforts to eliminate counterfeit and pirated items through ongoing business initiatives designed to reduce bad buyer experiences and improve customer satisfaction and by responding to new patterns we are seeing among counterfeiters and others committing fraud on our users. Notwithstanding these efforts, we believe that the legal climate, especially in Europe, is becoming more adverse to our positions, which may require us to take actions which could lower our revenues, increase our costs, or make our websites less convenient to our customers, any of which could materially harm our business. In addition, a public perception that counterfeit or pirated items are commonplace on our sites, even if factually incorrect, would damage our reputation, lower the price our sellers receive for their items and damage our business.

Content owners and other intellectual property rights owners may also seek to bring legal action against entities that are peripherally involved in the sale of infringing items, such as payment companies. To the extent that intellectual property rights owners bring legal action against PayPal based upon the use of PayPal's payment services in a transaction involving the sale of infringing items, including on our websites, our business could be harmed. Several jurisdictions have adopted new laws in these areas, and others are considering imposing additional restrictions.

In addition, new laws have been proposed regulating Internet companies with respect to intellectual property issues. For example, SOPA, which has been introduced in the U.S. House of Representatives, and PIPA, which has been proposed in the U.S. Senate, would give rights owners and the government broad powers to bring lawsuits against websites accused of enabling or facilitating copyright infringement, and such lawsuits could result in, among other consequences, payment providers such as PayPal being precluded from doing business with allegedly infringing sites, as well as search engines being precluded from linking to, and Internet service providers being required to block access to, such sites. In addition, the European Commission has reopened the Intellectual Property Enforcement Directive, which could potentially increase our exposure to enforcement actions from rights owners. Implementation of these or similar laws could require us to change our business practices, increase our compliance costs and harm our business."

SOPA and PIPA are now off the table in the U.S. On the other side of the Atlantic, the revision of

the Enforcement Directive remains on the agenda. We hope that new legal incentives can be found to induce a pro-active role for payment intermediaries when they benefit from obviously illicit trade run by third parties, while reassuring them they should not immediately bow when some politicians are just blaming websites which, as WikiLeaks, only contribute to the transparency of government. No double standard please! Please act in a consistent way if you do not want your reputation to be damaged!