H.R. 3261, STOP ONLINE PIRACY ACT

Introduced October 26, 2011

The Stop Online Piracy Act (H.R. 3261) builds on the Pro IP Act of 2008 and the Senate's PROTECT IP Act introduced earlier this year. The bill reflects a bipartisan and bicameral approach toward ensuring that law enforcement and job creators have the necessary tools to protect American intellectual property from counterfeiting and piracy.

RESPONDING TO MYTHS:

- ***Myth: Saying it creates an 'Internet Blacklist'*** – critics have charged that the bill could create an 'internet blacklist' that gives the "government dramatic new powers" to target websites providing infringing goods/services.
    - ***Fact*** – This bill ensures that first amendment rights and due process are protected. It is targeted toward websites engaged in facilitating criminal activity. Under existing law, the Attorney General has authority to take action against infringing websites hosted on domestic TLDs (top level domains). This bill fixes a loophole that currently excludes websites hosted on foreign TLDs.

- ***Myth: Saying that the bill would 'break the internet'*** – since domains could be blocked, that could require all third party sites to remove and disable links to the website and even target user generated content on social media sites.
    - ***Fact*** – The bill simply expands the Attorney General's existing authority to seek a court action to block infringing websites on domestic TLDs, to those on foreign TLDs. The bill has been carefully crafted to ensure that in those instances where a block order is issued it is limited to actions similar to what currently takes place on domestic TLDs and does not impose new burdens on social media and related user generated content. It does not require third party websites to scrub their sites and disable links.

- ***Myth: Saying that it 'short-circuits the legal system'*** – arguments have been made that the bill gives rights holders a fast track to shutting down infringing websites which somehow circumvents the U.S. legal system.
    - ***Fact*** – The bill allows only the Attorney General to seek, in certain extreme cases, an order from a federal judge to block a website on a foreign TLD, similar to authority that already exists for domestic TLDs.
    - ***Fact*** – No rights holder has the ability to seek an order to block or shut down a website. All that the rights holder can do is avail themselves of the two-part mechanism, which in the second part requires a federal judge to make a legal determination as to the status of an accused website.

- ***Myth: Saying that it creates conflicts between DNS servers*** – and that this would make people vulnerable to hackers, identity theft, and cyberattacks.
    - ***Fact*** – The bill provides law enforcement with the authority to investigate criminal activity. The provisions in the bill do not create a conflict between DNS servers; they simply close a loophole in existing law and ensure that the Attorney General can enforce the law against websites operating on foreign TLDs.
    - ***Fact*** – The bill also prohibits anti-circumvention technologies to protect consumers from unknowingly using foreign servers that could compromise their personal and financial information. Those who may choose to use such technologies to access servers in Russia or China do so knowing that their personal information may be compromised.

- ***Myth: Saying that the bill 'censors the internet'*** – since the government is taking action against infringing websites, this amounts to censorship, akin to what takes place in totalitarian countries.
    - ***Fact*** – First, the bill ensures that First Amendment rights and Due Process are protected. The First Amendment is not a cover for engaging in criminal activity. The infringing websites in question have ample opportunity to participate in judicial proceedings, if they choose to do so. The bill's actions are directed toward websites that are trafficking in illegal goods or copyrighted material.
    - ***Fact*** – There is an important distinction between free speech and the theft of goods or services. Censorship in oppressive regimes is about speech, freedom, and fundamental human rights. It is appalling and offensive to attempt to draw a parallel to political dissidents and those denied religious freedom to those who will no longer be able to make money from engaging in illegal activity and theft.

- ***Myth: Saying that the bill 'provides no recourse and remedy for harm by the website owner'*** – since intermediaries are incentivized to simply sever their relationship with a website in exchange for immunity.
    - ***Fact*** – First, an accused website owner has full and ample opportunity to make their case. This is not designed to be a one-sided procedure. If a rights holder brings a false claim against a website, then they will be on the hook for legal sanctions and damages.
    - ***Fact*** – Second, the intermediary is immunized whether they take action voluntarily or after a court order has been issued to the infringing website. If an intermediary is unable to complete their thorough review within the set time, there is no incentive for them to act rashly. The two-step mechanism is designed to ensure that there is thorough review and examination of a merchant website's activities before any action is taken.

- ***Myth: Saying that the bill 'creates a litigation and liability nightmare' for tech companies*** – by enacting a new regulatory framework.
    - ***Fact*** – The bill does not replace existing DMCA notice-and-takedown procedures that are used when infringing content is posted on legitimate websites.
    - ***Fact*** - It does create a new process for the Attorney General and rights holders to take action against illegitimate sites, those devoted to infringing activity and theft. These are websites that are actually being used and marketed to facilitate theft, not websites or other technologies that could simply have the potential of being misused.
    - ***Fact*** – This bill does not force Internet companies to police their user's activities. The bill is not intended to go after single pages or instances of infringing activity, and legitimate websites should not be under threat of losing their advertising and payment services. In fact, if a rights holder makes a false claim against a website, then they will face severe legal sanctions and will be on the hook for damages.

- ***Myth: Saying that the bill 'provides for monetary sanctions against intermediaries'*** – in so-called private rights of action.
    - ***Fact*** – For rights holders, this bill includes a clear two-part mechanism that does not provide a way for a rights holder to seek or collect monetary damages from an intermediary. It simply allows them to receive injunctive relief against the rogue website.
    - ***Fact*** – Once it becomes clear that a website is dedicated to infringing activity and the relationship between financial intermediaries and ad providers is severed, then the financial relationship with the party engaging in criminal theft of goods or services would obviously end.