Hidden in the Shadows:

Abuse of the 'Notice and Takedown' Mechanism

by Jayshendra Karunakaren

'Notice and takedown' systems are an essential working mechanism to implement copyright infringement laws worldwide. Essentially, such a system removes an internet service providers' (ISPs) secondary liability for hosting material that infringes the intellectual property rights holders. This is because ISPs are legally required to create a system that issues a "notice" (enforced by domestic law) to copyright infringers and "takedown" (remove) the copyright infringing-material.

In Thailand, The regulation issued by the Ministry of Digital Economy and Society (DE) (labelled the *Notice and takedown of computer data and the removal of computer data from computer systems*) on 22 July, 2017 mandates ISPs to issue takedown notices to online users who upload content that violates the latest version of the Computer-related Crimes Act. While notice and takedown systems in other countries' copyright infringement laws are a less obvious way of censoring information, Thailand's incorporation of the 'notice and takedown' system in combating online dissent is perhaps one of the most direct and clear examples of censorship relative to other countries.

Introducing the 'notice and takedown' systems at the international level

The creation of the 'notice and takedown' system is solely due to the creation of international copyright laws by the United Nation's World Intellectual Property Organization (WIPO). WIPO's Copyright Treaty sets provisions to better protect the woks and the rights of their authors in the digital environment. To implement WIPO's Copyright Treaty, the US Congress drafted and implemented online copyright legislation, termed as the Digital Millennium Copyright Act (DMCA). The US was the first country to create a stricter, more streamlined online copyright protections as the US has the highest number of worldwide ISPs and has the highest volume of internet traffic globally. The DMCA served as the model to be followed by other countries who began to adopt similar legal protections to comply with WIPO.

The first 'notice and takedown' system is found in Section 512 of the DMCA. The system is a bargain between copyright holders and ISPs to remove the secondary liability of ISPs while

at the same time, protecting copyrighted works from being pirated. This bargain is commonly known in legal terminology as the '*safe harbour*' provision (because ISPs cannot be held liable in court for hosting infringing material).

On the side of the ISPs, ISPs that host content (such as websites, forums, social networking profiles) and search engines do not face secondary liability for a material that infringes copyright on its platform, ie they should not be sued in court. On the side of the copyright holders, such ISPs are required to implement a system which receives notices from copyright holders alleging material that has been infringed, and "expeditiously" (define the legal problems with this word) respond to these notices of infringement by removing or disabling access to the infringing material.

In addition, if the users who upload the alleged infringing material wants to dispute the takedown of their content, they should be able to forward a counter-notice back to the original complainant. If after 10 to 14 days, the complainant has not notified the ISP that it has filed a lawsuit, then the ISP should reinstate the disputed material. This last provision is installed in the 'notice and takedown' system' to ultimately protects the freedom of expression of internet users.

The philosophy that underlies this bargain is that ISPs do not have any real knowledge of the infringement before they are issued with a notice from copyright holders. The general structure of this system has been copied in other countries.

Thailand new established system of 'Notice and Takedown'

The general structure of the system is similar to the standard model used in the US and in other countries. However, there are some unique elements to Thai system, such as the more active involvement of law enforcement agencies in validating the infringement claims, the absence of a standardized counter-notice channel for internet users, and the greater discretion possessed by ISPs in deciding whether the online material should remain in cyberspace. These differences have significant implications on free speech.

If you need more background information on 'notice and takedown', please read the *preceding article* (past hyperlink here).

The ‘notice and takedown’ system is firstly institutionalised within the revised Computer-related Crimes Act (CCA) by junta-appointed parliament. To implement the new provisions of the CCA, the Ministry of Digital Economy and Society has created a ‘notice and takedown’ regulation in July 2017, which will be explained as follows

Step 1: Lodging a complaint

If an individual intends to report an online material that he or she perceives to vioate Section 14 of the CCA, the individual should report the infringement to the police and provide documents and other evidence proving the offence to the law enforcement officials.

After that, the complainant should fill out the complaint form prepared by the ISP. Similar to WIPO’s Copyright Treaty and the US DMCA law, the ‘notice and takedown’ system in Thailand mandates that ISPs prepare a written boiler-plate form of a takedown notice. A copy of the police report would also have to be submitted to the ISPs along with the standardized notice form.

The notice must include:

(1) the contact details of the ISP, and
(2) a boiler-plate complaint form that can be used to issue notices bringing to light violations of Section 14 of the CCA. This complaint form would have to include:
- the name, address and signatures of the complainants,
- the details of the online information and its infringement against Section 14,
- contact information of the ISPs, including email, address, phone or fax numbers,
- an explanation of the damage inflicted on other users,
- a certification message validating that the information is true.

The preparation of a boiler-plate notice form by ISPs is also found in the DMCA. The only difference with the DMCA in this step is that in Thailand, the law enforcement agencies are involved from the start a copy of the police report is required to be submitted to the ISP.

Step 2: The ‘Takedown’

After receiving the complaint form, ISPs must remove the infringing material from its hosted space. In addition, the ISPs have to prepare a copy of the complaint and submit it to the original complainant.

The new regulation from Ministry of Digital Economy and Society has set strict time limits for the infringing material to be removed. The time limits are:

(1) online material violating Section 14(1) for false or distorted computer data must be removed within 7 days after the complaint has been received,
(2) online material violating Section 14(2) and (3) for computer data against national security must be removed within 24 hours after the complaint has been received, and
(3) online material violating Section 14(4) for obscenity must be removed within 3 days of the complaint being received.

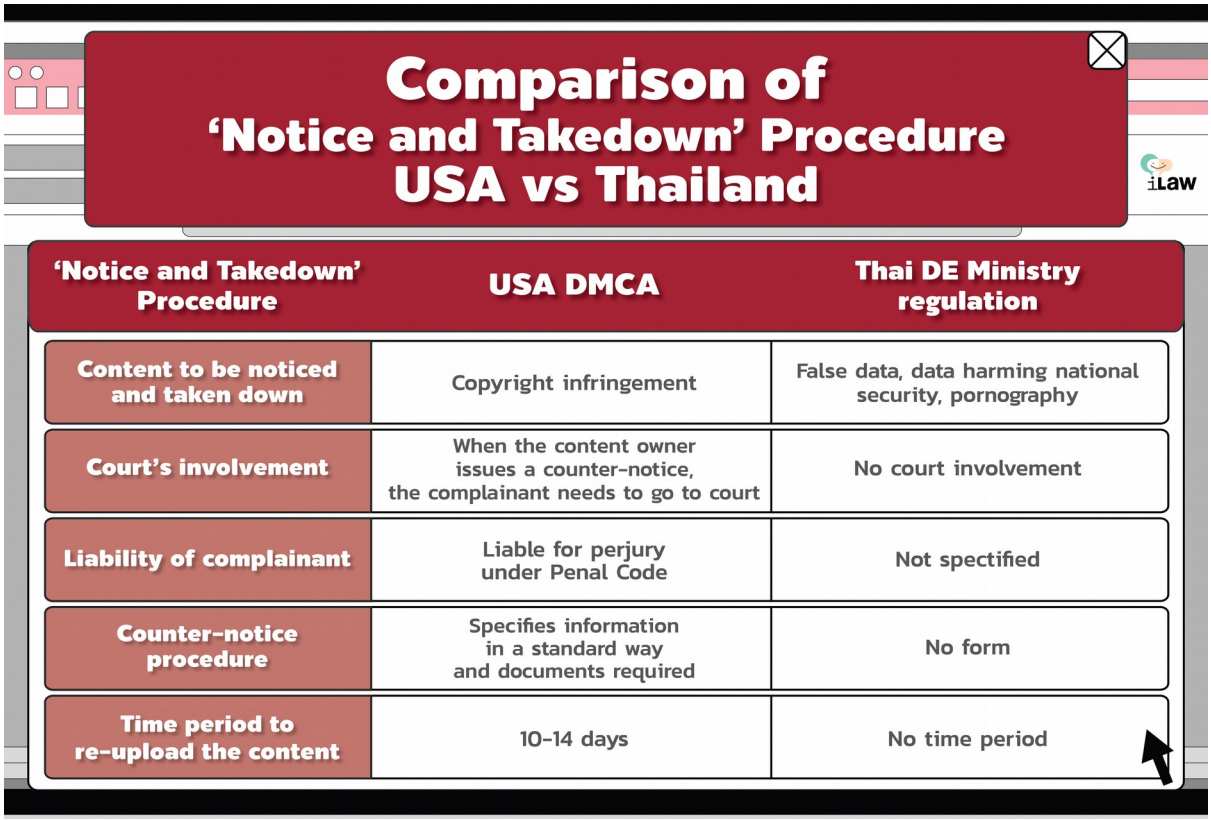
The specification of exact time limits for removal of the infringing online material is a unique element in the Thai system. WIPO's Copyright Treaty and the DMCA do not specify exact time limits for the ISP to remove an infringing material. The only provision in the DMCA governing the timeline is that ISPs should "expeditiously" remove the infringing material. While the word "expeditious" can be taken to be generally defined as "conducted with speed and efficiency", the US courts have not given an exact timeline that would qualify as "expeditious". Each dispute that has been tried by the courts have been judged on a case-by-case basis, and thus the timelines have been judged within the context of the facts to the dispute. Weeks and even months have been judged by the courts to qualify as "expeditious".

<u>Step 3</u>: Disputing the Takedown

The internet users who had their online material removed have the right to challenge the takedown by:

(1) Reporting the takedown to the police, with the details of the allegedly infringing material, the damage to the user, and other evidence proving that the material does not constitute an infringement to Section 14.
(2) Informing the ISP of their challenge to the takedown and submit a copy of the police report (in addition to other evidence). However, there is no boiler-plate counter-notice form available for the internet user.
(3) Once the ISP receives the challenge, it may re-upload the material back onto its hosted website or search index. However, this decision is completely up to the discretion of the ISP.

The procedures for disputing the takedown is quite different from the US context. First, the law enforcement agencies are involved once again. Second, there is no boiler-plate counter-notice that is available for use to the internet user. Third, and perhaps the most important, the ISPs have full discretion to decide whether to re-upload the content. In the US, ISPs are legally obliged to re-upload the content if the original complainant does not decide to dispute in court.



'Notice and Takedown' Procedure	USA DMCA	Thai DE Ministry regulation
Content to be noticed and taken down	Copyright infringement	False data, data harming national security, pornography
Court's involvement	When the content owner issues a counter-notice, the complainant needs to go to court	No court involvement
Liability of complainant	Liable for perjury under Penal Code	Not specified
Counter-notice procedure	Specifies information in a standard way and documents required	No form
Time period to re-upload the content	10-14 days	No time period

Investigating the abuse 'notice and takedown' through a foreign lens

The potential abuse to the system in Thailand will be analysed by studying the experience of the Digital Millennium Copyright Act (DMCA) in the US. This is observed through five ways:

(1) The 'notice and takedown' system excessively pressures ISPs into removing allegedly material without properly examining constitutes of the laws.

A big problem with the US DMCA 'notice and takedown' system is that ISPs are pressured to comply with a takedown notice from the copyright holders, without checking if the allegedly infringing material is a true copyright violation. If they fail to comply, they would face a huge risk facing a lawsuit for contributing to copyright infringement. This means that ISPs would remove allegedly infringing material without adequately examining. This has significant free speech implications as false takedown of material occurs frequently.

In addition, if the removed material owner does not have the resources or knowledge to issue a counter-notice, the material then stays removed despite the wrongful use of the DMCA. In the best-case scenario, if the online material is re-uploaded onto the internet after the dispute, it can only happen 10 to 14 days after the counter-notice was issued.

This excessive pressure is much worse in the Thai system. This is because the Ministry of Digital Economy and Society has set a strict, short time limits for the removal of online material that allegedly violates Section 14 of the Computer-related Crimes Act. It is unreasonable to expect that ISPs can conduct a thorough examination of the online material given that: such material may be lengthy, may be difficult to comprehend and that properly applying the provisions of Section 14 may require legal experts.

Thus, given the presence of these time limits in Thailand, the pressure exerted upon ISPs to remove online material without checking the validity of the legal exercise is multiplied, relative to the US. It is thus more likely that a wrongful takedown of online material may occur and this abuse of the law will be unchecked.

(2) The system does not afford judicial protection to the internet user.

The 'notice and takedown' system does not afford adequate protection from the courts for the internet user. In the US, judicial protection is only made available to the user only after three things happen a counter-notice is issued and the complainant files a lawsuit.

By comparison, there is no avenue for the involvement of the judicial review in Thailand. While in the US, the original complainant may have to insist their request in court, the procedure in Thailand is designed whereby the ISPs have the final say to decide whether the material should be uploaded onto its system.

This means that in most cases in both Thailand and the US, online material can be censored without the involvement of the courts to rule whether the application of the Computer-related Crimes Act (Thailand) and the DMCA (US) was legitimate and fair. As large proportion of cases do not involve the courts, judges and lawyers will have very few precedents to work with to develop a legal interpretation. There is very little transparency to the public over how the 'notice and takedown' system is applied. Thus, other internet users will most probably not have adequate information to understand and exercise their rights under this procedure.

(3) Internet users are not protected from false allegations of offense.

Studies of DMCA conducted by the *Chilling Effects* and *The Takedown Project* research groups shows that a large sample of takedown cases in the US has been removed illegitimately. The liability for an incorrect takedown under the DMCA rest with the

complainant, as the complainant must issue a notice under the legal penalty of perjury. This also harms the true copyright holder who rely on the dissemination of their works to the public.

However, the situation in Thailand is much trickier than the US. This is because knowing what constitutes an actual offense requires determining what constitutes '*truth*' and '*falsity*'. Section 14(1) and (2) of the Computer-related Crimes Act state that any '*false*' computer data that is imported into a computer system that causes damage to a third party, the public, the country's security, or cause a public panic constitutes an offense. It is very complicated when analysing the 'truth' and 'falsity' of general comment or criticism. Any perception, view, and/or expression is open to interpretation in many ways, especially regarding comments of an anti-government nature.

(4) The procedure for issuing a counter-notice disadvantage small internet users.

This is a feature of the inequality of the US and Thai system. In the US, a valid counter-notice must contain physical or electronic signature, identification of the removed material and its former location, statement under penalty of perjury, contact details of the user, and consent to the jurisdiction of the Federal Court. The Thai system of issuing a counter-notice involves submitting a police report (along with supporting evidence used to lodge the report) and a statement informing the ISP that the user intends to dispute the takedown.

This problem is even worse in Thailand as there are no standard counter-notice form, which means that it is probable that a high number of internet users intending to dispute a takedown will submit a counter-notice issue that does not fulfil the standard criteria without exact knowledge on the laws.

(5) There is no time period as to when the material can be re-uploaded

In the US, regardless of the legitimacy of the counter-notice from the internet user, the ISP can only restore the material on the hosting website after 10 to 14 days. This waiting period where the material is not published online can lead to certain damages. For example, some public information would be crucial in the time leading up to events of national importance, owners who rely on online distribution of his or her work to gain recognition can face major problems. Even if the material is restored online after the waiting period, irreparable damage could have already been done to the internet users' reputation.

These same damages would be even worse in Thailand as there is no time specification as to when the material can be re-uploaded, as the waiting period is likely arbitrary.